Government of Canada
Canadian General Standards Board

Gouvernement du Canada
Office des normes générales du Canada

CAN/CGSB-72.34-2017

Supersedes CAN/CGSB-72.34-2005

National Standard of Canada

Electronic records as documentary evidence

Canadian General Standards Board CGSB

Standards Council of Canada
Conseil canadien des normes

Canada

Experience and excellence
Expérience et excellence
CGSB ONGC

The CANADIAN GENERAL STANDARDS BOARD (CGSB), under whose auspices this standard has been developed, is a government agency within Public Services and Procurement 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 of Canada, 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 and Procedures Manual for the Development and Maintenance of Standards.

CGSB standards are subject to review and revision to ensure that they keep abreast of technological progress. CGSB will initiate the review of this standard within five years of the date of publication. 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 at our Web site — www.tpsgc-pwgsc.gc.ca/ongc-cgsb/index-eng.html along with more information about CGSB products and services.

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 is entirely their own responsibility.

Language
In this Standard, “shall” states a mandatory requirement, “should” expresses a recommendation and “may” is used to express an option or that which is permissible within the limits of this Standard. Notes accompanying clauses do not include requirements or alternative requirements; the purpose of a note accompanying a clause is to separate from the text explanatory or informative material. Annexes are designated normative (mandatory) or informative (non-mandatory) to define their application.

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

The Manager
Standards Division
Canadian General Standards Board
Gatineau, Canada
K1A 1G6

A National Standard of Canada is a standard developed by an SCC-accredited Standards Development Organization (SDO), and approved by the Standards Council of Canada (SCC), in accordance with SCC’s: *Requirements and Guidance-Accreditation for Standards Development Organizations, and Requirements and Guidance-Approval of National Standards of Canada Designation*. More information on National Standard requirements can be found at www.scc.ca.

An SCC-approved standard reflects the consensus of a number of experts whose collective interests provide, to the greatest practicable extent, a balance of representation of affected stakeholders. National Standards of Canada are intended to make a significant and timely contribution to the Canadian interest.

SCC is a Crown corporation within the portfolio of Industry Canada. With the goal of enhancing Canada’s economic competitiveness and social well-being, SCC leads and facilitates the development and use of national and international standards. SCC also coordinates Canadian participation in standards development, and identifies strategies to advance Canadian standardization efforts. Accreditation services are provided by SCC to various customers, including product certifiers, testing laboratories, and standards development organizations. A list of SCC programs and accredited bodies is publicly available at www.scc.ca.

Users should always obtain the latest edition of a National Standard of Canada from the standards development organization responsible for its publication, as these documents are subject to periodic review.

The responsibility for approving standards as NSCs rests with:

Standards Council of Canada
55 Metcalfe Street, Suite 600
Ottawa, Ontario K1P 6L5, CANADA

How to order CGSB Publications:

by telephone — 819-956-0425 *or*
— 1-800-665-2472

by fax — 819-956-5740

by mail — CGSB Sales Centre
Gatineau, Canada
K1A 1G6

in person — Place du Portage
Phase III, 6B1
11 Laurier Street
Gatineau, Quebec

by email — ncr.cgsb-ongc@tpsgc-pwgsc.gc.ca

on the Web — www.tpsgc-pwgsc.gc.ca/ongc-cgsb/index-eng.html

NATIONAL STANDARD OF CANADA **CAN/CGSB-72.34-2017**

Supersedes CAN/CGSB-72.34-2005

Electronic records as documentary evidence

CETTE NORME NATIONALE DU CANADA EST DISPONIBLE EN VERSIONS FRANÇAISE ET ANGLAISE.

ICS 37.080

Published March 2017 by the
Canadian General Standards Board
Gatineau, Canada K1A 1G6

CANADIAN GENERAL STANDARDS BOARD

Committee on Electronic Records and Image Management

(Voting membership at date of approval)

Chair (Voting)

Duranti, L.	Interpares Trust (General interest)

General interest category

Fox, U.	Arma Canada
Groulx, K.	The Advocates Society
Lachance, M.	Mindshare Consulting Services
Spiteri, L.	Dalhousie University

Producer category

Caughell, T.	Open Text Corporation
Davis, R.G.	Data Repro Com Limited
Knight, S.	Access Systems Ltd.
Krishnamoorthy, R.	Deloitte LLP
Knoppers, J. V.	Information Management Services (Infoman) Inc.
Priest, G.	Iron Mountain
Peterson, V.	CriticalControl Solutions

Regulator category

Cooper, R.	Treasury Board of Canada Secretariat
Jahn, C.	Canada Border Services Agency
Tremblay, G.	Canada Revenue Agency

User category

Banks, T.	Public Services and Procurement Canada
Ball, J.	Royal Canadian Mounted Police
Curley, D.	Privy Council Office
Earle, H.	Agriculture and Agri-Food Canada
Gourlie, M.	Association of Canadian Archivists
Laferrière, H.	Data Management Association (DAMA)
Meldrum, A.	Innovation, Science and Economic Development Canada
Stephens, S.	Canadian Bankers Association

Secretary (non-voting)

Lozano, A.	Canadian General Standards Board

Acknowledgment is made to Brian Thurgood and Lois Evans for leading the working group in the revision of this standard.

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

Contents Page

Foreword

CAN/CGSB-72.34 specifies principles, methods, and practices for the creation (i.e. making, receipt, and capture) and management of all forms of electronic records (e.g. e-mail, cartographic, audio-visual, textual, multimedia, etc.) to support their admissibility (see 3.5 and 3.6) and weight (see 3.74) as evidence in legal proceedings. Because this standard provides only general legal, management and technical information, users should seek expert advice before applying its recommendations to specific records or systems.

This standard is harmonized with applicable federal, provincial and territorial acts in force and their pursuant regulation at the time of the Committee's deliberations. Where differences exist between an act or a regulation and this standard, the former shall prevail.

0 Introduction

0.1 About this standard

An organization may be required to produce electronic records as evidence in legal proceedings. To support the admissibility and weight of electronic records as documentary evidence, the organization needs to ensure that these records can be proven or presumed to be reliable, accurate, and authentic, that is, trustworthy. To ensure the trustworthiness of their electronic records, an organization should comply with this standard.

This standard uses the term “electronic record” rather than “digital record.” Whereas the term “digital record” refers to a record composed of discrete binary values aggregated into one or more bit stream, the term “electronic record” encompasses any digital record as well as any analogue record that is carried by an electrical conductor and requires the use of electronic equipment to be made intelligible to an individual.

This standard is information technology agnostic, in that it neither assumes nor endorses any specific system environment, database management system, database design paradigm, system development methodology, data definition language, command language, system interface, user interface, syntax, computing platform, or any technology required for implementation. This standard supports an integrated, interoperable electronic records management system approach.

This standard provides a framework and guidelines for the implementation and operation of records systems for electronic records, whether or not any information held therein will ever be required as evidence. Thus, compliance with it should be regarded as a demonstration of responsible business management. Applying the standard to an organization’s business will not eliminate the possibility of litigation, but the probability is that it will make the production of electronic records easier and their acceptance in a legal procedure more certain.

0.2 Relationship to Canadian legal evidentiary requirements

Records recorded by or stored in an electronic technology may be admissible as evidence in Canadian legal proceedings. If their admissibility is challenged, the records will need to satisfy certain statutory and, in some cases, common law admissibility requirements. These requirements may vary depending on the purpose for which the records are offered into evidence. 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 Use of this standard in legal proceedings

In legal proceedings, this standard could inform the development of arguments about the definitions of the key phrases of the rules of admissibility for electronic records. These phrases are “IT system integrity” and “record integrity,” as used in the electronic record provisions of the Evidence Acts, and records “made in the usual and ordinary course of business” as used in the CEA.

0.4 Terms and definitions

This standard uses terms and definitions derived from relevant national and international standards, guidelines, and policies.

0.5 English and French versions of this standard

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 from the international French for some terms, because of Canadian usage. For example, the terms “final disposition,” “preservation,” “record,” and “records management” in the English version are translated as “élimination,” “préservation,” “enregistrement,” and “gestion des enregistrements” respectively.

Supersedes CAN/CGSB-72.34-2005

Electronic records as documentary evidence

1 Scope

1.1 This standard provides guidance for developing policies, procedures, processes and documentation that support the continuing reliability, accuracy and authenticity of electronic records to:

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

b) support the admissibility and the weight of electronic records in legal proceedings; and

c) protect the capability of electronic records to effectively document an organization's decisions, actions, and transactions and to hold accountable those who are responsible for them.

1.2 This standard applies to organizations that make, receive, capture, maintain, manage, use, transmit, dispose or store recorded information electronically, and to private and public sector activities, irrespective of whether such activities are undertaken on a for-profit or not-for-profit basis.

1.3 This standard is intended to ensure that electronic records in records systems are trustworthy. Typical users include

a) managers of private and public sector organizations;

b) IT systems and records management professionals;

c) legal professionals and those responsible for security services and risk management; and

d) other individuals responsible for creating (i.e. making or receiving, or storing) and maintaining an organization's records.

1.4 This standard outlines methods for the management and preservation of electronic recorded information that are regarded as best practices independently of legal considerations. Therefore, organizations conforming to this standard benefit even when evidentiary issues are not in question.

1.5 In addition, this standard provides guidelines for

a) a procedural framework supporting quality practices in records management; and

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

2 Normative references

The following normative documents contain provisions that, through reference in this text, constitute provisions of this National Standard of Canada. The referenced documents may be obtained from the source noted below.

NOTE The addresses provided below were valid at the date of publication of this standard.

An undated reference is to the latest edition or revision of the reference or document in question, unless otherwise specified by the authority applying this standard. A dated reference is to the specified revision or edition of the reference or document in question.

2.1 Department of Justice

Canada Evidence Act (CEA)

Personal Information Protection and Electronic Documents Act (PIPEDA).

2.1.1 Source

The above may be obtained from the Department of Justice Canada, Communications Branch, Public Affairs Division, 284 Wellington Street, Ottawa, ON K1A 0H8, Telephone 613-957-4222, Facsimile 613-954-0811, Web site http://canada.justice.gc.ca.

2.2 Evidence Acts of each provincial and territorial jurisdiction may be obtained from their respective Justice Laws Websites.

2.3 Other sources considered in the development of this standard are listed in Annex A.

3 Terms and definitions

For the purposes of this National Standard of Canada, the following terms and definitions apply.

3.1
access
right, opportunity, or means of finding, consulting or retrieving **recorded information**.

3.2
access control
process of allowing only authorized individuals to have **access** to records in the **records system**.

3.3
accountability
principle that individuals and organizations, being responsible for their actions, may be required to provide an account of them.

3.4
accuracy
degree to which **recorded information** is precise, correct, truthful, free of error or distortion.

3.5
admissibility (records)
capability of **recorded information** to be introduced as **evidence** in a legal proceeding.

3.6
admissibility (rules)
rules by which records are judged to be acceptable as evidence in legal proceedings.

3.7
analogue record
record written on physical material, such as a paper, parchment, stone, clay, film or certain types of magnetic audio- and videotape.

See also 3.51, record.

3.8
audit
systematic review of **recorded information** activities for compliance with policies, procedures, and controls are established and complied with to meet all financial, operational, legal, and regulatory obligations.

3.9
audit trail
log of IT system activities that enables the reconstruction, reviewing and examination of the sequence of activities relating to an operation, a **procedure**, or an event in a transaction.

3.10
authentic record
record that is what it purports to be and that is free from tampering or corruption.

3.11
authentication
declaration of **authenticity** at a given point in time.

3.12
authenticity
quality of an entity that it is what it purports to be and that it is free from tampering or corruption.

3.13
authorized individual
individual who is given a specific responsibility by a higher authority who has the power to do so.

3.14
backup (copy)
an exact copy of active electronic systems, programs and data made for the purpose of recovery in the event of a system problem or disaster.

3.15
capture
act of recording or saving a particular instance of **recorded information**.

3.16
cloud computing
model for enabling ubiquitous and on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.

3.17
conversion
process of changing **recorded information** from one format to another.

See also 3.42, migration.

3.18
copy
duplicate of **recorded information**.

3.19
data
smallest meaningful units of **recorded information**.

3.20
destruction (records)
process of eliminating **records** beyond any possibility of reconstruction.

3.21
digital
representation of an object or physical process through discrete, binary values.

3.22
digitization
process of rendering analogue **recorded information** in electronic (digital) form.

See also 3.7, analogue record.

3.23
disk image
bit-by-bit reproduction of the storage **medium** and its content including ambient **data**, swap space, and slack space.

3.24
disposition (records)
action taken on **records** after expiration of the **records retention period**, i.e. **destruction**, **transfer** or **preservation**.

3.25
document
indivisible unit of **recorded information** having stable content and fixed form.

3.26
documentary evidence
recorded information admitted as **evidence** in legal proceedings.

3.27
electronic discovery (e-discovery)
pre-trial procedure requiring an exchange of relevant **electronic records** among the parties.

3.28
electronic information
any **recorded information** that is carried by an electrical conductor and requires the use of electronic equipment to be intelligible by a person.

3.29
electronic record
an analogue or digital record that is carried by an electrical conductor and requires the use of electronic equipment to be intelligible by a person**.**

See also 3.51, record and 3.7, analogue record.

3.30
encryption
conversion of **recorded information** into a secret code (or plain text into cipher text).

3.31
evidence
all means by which any alleged matter of fact, the truth of which is submitted to investigation, is established or disproved in a legal proceeding.

3.32
format
means of encoding **data** to contain **information** about its structure, organization, and content so that it can be interpreted for future use in storage, retrieval, processing, presentation, manipulation, and transmission activities.

3.33
hearsay
out-of-court statement by someone other than the individual who is testifying and which is submitted for the truth of the facts in the statement.

3.34
information
message intended for communication.

3.35
information security
multidimensional discipline designed to keep **recorded information** in all locations free from any threat by a combination of mechanisms (technical, organizational, human-oriented, and legal).

3.36
IT system
set of one or more computers, associated software, peripherals, terminals, human operations, physical processes, information transfer means, that form an autonomous whole, capable of performing information processing and/or information transfer.

3.37
IT system integrity
proven capability of an **IT system** to perform its intended functions in an unimpaired manner, free from unauthorized manipulation, whether intentional or accidental, and the fact that it did so when the **recorded information** was generated and used.

3.38
IT system reliability
quality of a system that has been tested, subjected to peer review or publication, accepted within the relevant scientific community and whose known or potential error rate is acceptable.

3.39
legal hold
process whereby an organization preserves all forms of potentially relevant **records** when litigation is reasonably anticipated or underway.

3.40
medium
material support to which the **recorded information** is affixed.

3.41
metadata
attributes that identify a **record** and describe its use, management, custodial history, and technological changes.

3.42
migration
process of moving **recorded information** from one **IT system** configuration to another.

See also 3.17, conversion.

3.43
official record
instance of a **record** that has the force of an **original record** and is authoritative, final, and complete.

3.44
organization
entity capable of having legal rights and duties.

3.45
original record
first complete **record** capable of reaching the purposes for which it was intended (i.e. effective).

NOTE An original record has three characteristics: primitiveness (i.e., the first to be generated); completeness; and effectiveness.

3.46
preservation (records)
whole of the principles, policies, and strategies that controls the activities designed to ensure the **records'** physical and technological stabilization and protection of intellectual content through time.

3.47
probative value
weight or credibility given to **evidence**.

See also 3.74, weight.

3.48
procedure
body of written and unwritten rules governing the conduct of a transaction, or the formal steps undertaken in carrying out a transaction.

3.49
process
series of motions, or activities in general, carried out to move towards each formal step of a **procedure**.

3.50
quality assurance (records)
procedures for monitoring and assessing the records system, aiming to maintain a desired level of quality.

3.51
record
any **document** made or received by an organization in the course and by reason of its activity, and kept for further action or reference.

3.52
record identity
whole of the attributes of a **record** that together uniquely identify it and distinguish it from any other **record.**

NOTE With **record integrity**, a component of **authenticity**.

3.53
record integrity
quality of being complete and unaltered in all essential respects.

NOTE With **record identity**, a component of **authenticity**.

3.54
recorded information
information affixed to a **medium** in a stable form.

3.55
recordkeeping
capture, storage, use, maintenance and disposition of **records** and their **metadata**.

3.56
records classification
systematic organization of **records** in groups or categories according to methods, procedures, or conventions represented in a plan or scheme.

3.57
records disposition
final action taken on a **record** that has met its prescribed retention period.

3.58
records lifecycle
model of **records management** and archival science that characterizes the life span of a **record** in sequential stages: creation or receipt; classification; maintenance and use; appraisal; **disposition** through **destruction** or transfer to an archival institution or agency; description in archival finding aids; **preservation**; and reference and use.

3.59
records management
field of management concerned with the creation (making, receiving or capturing), maintenance, use and **disposition** of **records**.

3.60
records management manual
document that defines the scope of the **records management** program, its authority, the services it provides, and the fundamental **records management** concepts.

3.61
records management system
structured process, based on records management principles, controlling the management of records associated with the business of an organization.

3.62
records preservation system
electronic system that maintains **electronic records** during and across different generations of technology over time.

3.63
records retention period
specified period of time that **records** are kept to meet operational, legal, regulatory, fiscal or other requirements.

3.64
records system
whole of an organization's **records**, and the **records management** and **records** preservation systems that control them.

3.65
reliability
quality of a **record**, the content of which can be trusted as a full and accurate representation of the transactions, activities, or facts to which it attests.

3.66
risk assessment
evaluation of the probability of an adverse event and of the extent of its impact to prepare for it.

3.67
secure electronic signature
electronic signature that results from the application of a technology or process prescribed by the *Secure Electronic Signature Regulations* (SOR/2005-30) made under subsection 48(1) of the PIPEDA.

3.68
source record (digitization)
analogue **record** from which an electronic (digital) **copy** is made.

See also 3.7, analogue record.

3.69
spoliation
act of destroying, altering or concealing evidence.

3.70
transfer (records)
giving the physical, legal and intellectual control of the **records** to another organization.

3.71
transitory record
record that does not need to be retained to meet operational, legal, regulatory, fiscal or other requirements.

3.72
trustworthy record
record that is accurate, reliable and authentic.

3.73
trustworthy system
records system that has **reliability** and integrity.

3.74
weight (of evidence)
credibility or **probative value** of **evidence**.

4 Acronyms and abbreviated terms

The following acronyms and abbreviations are used in this standard:

BYOC	Bring Your Own Cloud
BYOD	Bring Your Own Device
CEA	Canada Evidence Act
COBO	Corporate Owned Business Only
COPE	Corporate Owned Personally Enabled
CSP	Cloud Service Provider
EDI	Electronic Data Interchange
IT	Information Technology
RM	Records Management
RO	Records Officer
TAR	Technology Assisted Review

5 Legal requirements for electronic records as documentary evidence

5.1 General

Sections of the *Canada Evidence Act* (CEA) cited below apply only to legal proceedings governed by federal laws. There are comparable provisions in the laws of the provinces and territories for legal proceedings governed by the laws in those jurisdictions.

A records system may include:

a) original paper records, admissible as business records under provisions such as s. (section) 30 of the CEA;

b) electronic records, admissible under provisions such as s. 31 of the CEA;

c) microfilmed, digitized, or imaged records, admissible under the copy provisions such as s. 30 of the CEA, or the electronic records provisions such as s. 31 of the CEA;

d) “relied upon printouts” of electronic records, admissible under provisions such as subs. 31.2(2) of the CEA; or

e) records created through EDI (electronic data interchange), admissible under provisions such as s. 31 of the CEA.

Because the laws and standards governing the admissibility as evidence of electronic and paper records differ, their management may also differ. The laws of evidence applying to legal proceedings in the federal and provincial/territorial jurisdictions permit electronic documents (or records), including electronic images, to stand in the place of original paper source records, or their copies. To be admissible, an electronically-produced record of any kind shall satisfy the electronic record provisions of the law in the jurisdiction involved.

The primary principle advanced by this standard is that an organization shall always be prepared to produce its records as evidence. Continuous compliance with this standard is an essential part of the proof of the integrity of an electronic record or records system. Intermittent compliance may be better than no compliance, but it is not enough to prove the integrity. Therefore, compliance obtained only when legal proceedings are anticipated or are underway is not sufficient.

5.2 Requirements for admissibility of electronic records as documentary evidence

Use of an electronic record as evidence requires proof of the authenticity of the record, which can be inferred from the integrity of the electronic records system in which the record is made or received or stored, and proof that the record was “made in the usual and ordinary course of business” or is otherwise exempt from the legal rule barring hearsay (see s. 30 of the CEA for example).

5.2.1 Authenticity of the record

A record submitted as evidence shall be authenticated by providing evidence external to the record itself (e.g., the testimony of a witness to the making of the record) that it is what it purports to be (its identity and integrity are intact), see s. 31.1 of the CEA. This is the authentication rule. Alternatively, a record can be declared authentic if the integrity of the records system in which the record was made or received, or stored, and/or the reliability of the recordkeeping processes, can be proven.

5.2.2 Integrity of the electronic records system

If a party offers a record into evidence to prove the truth of its content, the best evidence rule applies. The best evidence rule prefers the original of a record (or primary evidence) over its copies (or secondary evidence). If the party offering the secondary evidence can satisfactorily explain the absence of the primary evidence so as to refute any suggestion of fraud, then the secondary evidence is admissible. With electronic records, the application of the best evidence rule is problematic due to the absence in the digital environment of what is traditionally considered an original. Therefore the law of evidence provides that the best evidence rule can be satisfied by proof of the integrity of the records system, as in subs. 31.2(1)(a) of the CEA.

Such "integrity" is proven, in the absence of evidence to the contrary, by evidence that

a) the electronic records system was at all material times 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 system. (e.g. subs. 31.3(a) of the CEA); or

b) the electronic record was recorded or stored by a party who is adverse in interest to the party seeking to introduce it into evidence (e.g., subs. 31.3(b) of the CEA); 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 was not under the control of the party seeking to introduce it (e.g., subs. 31.3(c) of the CEA).

5.2.3 "Record made in the usual and ordinary course of business"

If a party offers a record into evidence, for the proof of its contents, the hearsay rule also applies (see 3.33). An exception to the hearsay rule is made for business records on the assumption that organizations would use records procedures which ensure the reliability of the recorded information. The business records exception to the hearsay rule is satisfied by proof that the record in question was "made in the usual and ordinary course of business" of the organization from which the record comes (e.g., s. 30 of the CEA). The term "business" is given a wide definition to include, "any business, profession, trade, calling, manufacture or undertaking of any kind carried on in Canada or elsewhere whether for profit or otherwise" (e.g., subs. 30(12) of the CEA).

Just as is the case with the authentication rule and the best evidence rule, the application of the business records exception to the hearsay rule relies on proof of the integrity of the records system in which the record submitted as evidence was made or received or stored.

5.2.4 Proof of the integrity of an organization's records system

The following factors can be used to prove the integrity of an organization's electronic records system:

a) sources: the origin of the data in its electronic records is known;

b) contemporaneous recording: the electronic records are made or received or stored within a reasonable time after the events to which they relate, or stored within a reasonable time after they are received;

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 entry procedures are part of the usual and ordinary course of business of the organization, and are carried out in compliance with the RM manual and IT system management guide (see 6.4 and 6.5);

e) standards: the organization complies with applicable electronic records management standards as per 6.3.2. b);

f) decision making: the organization, when making decisions, relies upon the electronic records in its electronic records system;

g) software: the organization's software reliably operates the electronic records system and processes its data;

h) system changes: a record of record system changes and alterations is kept;

i) privacy: the use of the data in the organization's electronic records complies with the relevant Canadian, provincial and territorial privacy statutes governing the collection, use or disclosure of personal information, confidential commercial information, trade secrets, privileges or other confidential information; and

j) security: security procedures, such as protection against unauthorized access and disaster recovery plans, are used to guarantee the integrity of the electronic records system.

Proof of these factors is provided by the manual (section 6.4) and the IT system management guide (section 6.5).

5.3 Electronic discovery (e-discovery) and litigation preparedness

Electronic discovery is a pre-trial procedure in civil litigation requiring an exchange of relevant electronic records among the parties. Investigations and inquiries also involve the collection and production of electronic records, sometimes in very large numbers. There is a parallel system to civil law discovery for disclosure in criminal law proceedings involving pre-trial applications, the preliminary inquiry and *voir dire* hearings held during trial. The huge volumes, varying formats and volatility of electronic records present a number of challenges.

The first challenge is the identification of potential sources of relevant information. Organizations with a well-managed electronic records system will be able to find, preserve and collect relevant records much more quickly, accurately and cost-effectively than those whose electronic records are disorganized. As a result, electronic records management should be in place long before the need to perform e-discovery arises. A second challenge, in terms of time and expense, is record review and processing of records, which is increasingly being done using automated computer systems. More and more, e-discovery requires the review of thousands of records for relevancy and privilege. This review is increasingly being done with the assistance of machine learning (technology-assisted review, or TAR). Organizations that are in a position to efficiently collect only those records that are relevant (for example, by record type, record date, author/recipient or subject matter), will benefit from the reduced cost of review. A third challenge is for organizations to produce the relevant electronic records required by the court so that these records can be admissible as evidence in the legal proceedings. For more information, for e-discovery in civil litigation see the *Sedona Canada Principles*[1] and for disclosure in criminal law proceedings see R. v. Oler, 2014 ABPC 130 (CanLII).

5.3.1 Technology-Assisted Review (TAR) and other automated tools and techniques

Organizations may require their legal team and Record Officer (RO) to use Technology-Assisted Review (TAR) to meet the requirements of e-discovery. Methods using TAR are varied and may include: probabilistic search models, based on word interrelationships, proximity, and frequency; fuzzy search models, based on the core component of each word to capture all its possible forms; cluster search models, based on examination of groups of documents having similar content; and search categorization models that rely on a thesaurus. The TAR applications are equally varied, ranging from auto-categorization systems, de-duplication systems, email threading and predictive coding, to visual analysis.

However, courts may differ in their opinions as to the accuracy of such devices. For information on how to conduct e-discovery using TAR, see the *Sedona Canada Principles.*

5.4 Legal hold

Principle 3 of the *Sedona Canada Principles* states: "As soon as litigation is reasonably anticipated, the parties must consider their obligation to take reasonable and good-faith steps to preserve potentially relevant electronically stored information." The obligation to preserve recorded information arises as soon as litigation is contemplated or threatened. However, as to when that point is reached is an issue requiring legal advice. It can be difficult to assess in the early stages of a dispute. Such steps taken too early may involve disproportionate cost and effort. But delay

[1] *Sedona Canada Principles* is the title of a project of the Sedona Conference Working Group 7, Sedona Canada. "Sedona" is a reference to Sedona, Arizona, where the Sedona Conference is located. A pdf copy of *The Sedona Canada Principles* may be downloaded from Sedona Canada Principles site at http://goo.gl/woLSFh.

in imposing a legal hold upon normal disposal procedures can result in evidence being lost and consequently, penalties for spoliation. Therefore, a “good faith” assessment, based upon legal advice, should be carried out.

Notice of the need to impose a legal hold by preserving records in both paper and electronic form, should be given to all affected parties, including relevant non-parties and one’s own IT and records management staff. Such notice should provide clear instructions and details regarding the kinds of information that shall be preserved. It should be regularly re-sent and records custodians informed when such preservation requirements are lifted.

The records system shall have the capability to suspend the disposition of records (and all other recorded information) subject to a legal hold, audit, review, investigation, inquiry, access to information request or other legal or administrative proceeding. The RO, in consultation with the legal adviser, IT, and business managers, shall develop and implement a detailed, written legal hold procedure that defines among other things:

a) the individual or position within the organization who is authorized to issue, modify, and rescind a legal hold;

b) the process of co-ordination with the organization’s legal advisers;

c) the process for managing the legal hold and ensuring compliance;

d) the process by which custodians and data sources will be appropriately identified;

e) the IT systems vital to the legal hold;

f) the protection of the records from unauthorized access or modification; and

g) the actions taken to document the legal hold process.

The procedure shall include staff training on how to implement and manage the legal hold, and administer it without attracting sanctions for spoliation. The procedure shall emphasize that courts have a number of options to sanction a party which spoliates relevant evidence. These can include:

a) order the detention, custody, or preservation of evidence;

b) draw an adverse inference against a party guilty of spoliation;

c) refuse to admit evidence;

d) refuse to hear witnesses;

e) refuse to permit a party to examine or cross-examine a witness;

f) levy court costs against a spoliator;

g) impose a contempt of court order upon a spoliator; or

h) impose default judgment or dismiss the case (the court action).

Where there is concern that relevant evidence will not be preserved, a court can order that a party to legal proceedings be allowed to copy or take custody of evidence in the possession of another party.[2]

For these reasons, legal hold is potentially the responsibility of every individual within the organization.

[2] Such a court order is called an “Anton Piller order.” It is used for example, “when it is essential that the plaintiff should have inspection so that justice can be done between the parties… [and] there is a grave danger that vital evidence will be destroyed.” In *Celanese Canada Inc. v. Murray Demolition Corp.*, [2006] 2 S.C.R. 189, 2006 SCC 36, the Supreme Court of Canada provided guidelines for the granting and execution of Anton Piller orders.

5.5 Signatures

5.5.1 Electronic signature

Provisions of the CEA and the PIPEDA govern the use of electronic signatures in federal law. There are comparable provisions in the laws of the provinces and territories for electronic signatures. The function of a signature ─ to link a person with a document ─ is the same for a signature on paper or a signature associated with an electronic document. The requirement for a signature by a person is satisfied if the method used uniquely identifies the person and indicates the person's approval of the electronic record, and if the method used is reliable and appropriate in all the circumstances and includes agreement among the parties. It is generally accepted that "approval" means only willingness to adopt the text as one's own, without necessarily restricting a signature to one used to assent to a contract. Therefore, an "electronic signature" can mean electronic information that a person creates or adopts in order to sign a document and that is in, attached to or associated with, the document.

Under PIPEDA, a secure electronic signature means an electronic signature that results from the application of a technology or process which it can be proved that:

a) the electronic signature resulting from the use by a person of the technology or process is unique to the person;

b) the use of the technology or process by a person to incorporate, attach or associate the person's electronic signature to an electronic document is under the sole control of the person;

c) the technology or process can be used to identify the person using the technology or process; and

d) the electronic signature can be linked with an electronic document in such a way that it can be used to determine whether the electronic document has been changed since the electronic signature was incorporated in, attached to or associated with the electronic document.[3]

5.5.2 Wet signature

Where there is a requirement to maintain records with wet signatures (i.e. signatures made on the physical document using physical means) to provide evidence of approval, authorization, acknowledgement, verification, notarization or the witnessing of an act, such requirement can be satisfied by digitizing the record and maintaining a digital image of it, provided that all of the conditions set out for the digitization of paper records have been met. Because the legal, management, and technical information provided by this standard is general, users should seek expert advice before applying its recommendations to a specific records or IT system.

5.6 Authenticated paper copies for legal proceedings

Whenever paper copies of electronic records need to be produced, they shall be authenticated as true copies of the electronic records to support their admissibility and weight as evidence in legal proceedings. The procedures for producing and authenticating paper copies shall be documented.

The procedure for producing a paper copy of an electronic record shall require the use of an authorized individual's signature to authenticate the paper copy and to provide proof of authenticity when required to do so. Where the paper copy differs in structure, form, or content from the electronic record, the nature of the differences, their causes, and the manner in which they occur shall be documented in the authentication record (e.g. affidavit).

[3] See s. 48(2) of the PIPEDA and its Secure Electronic Signature Regulations (SOR/2005-30). See also s. 31.8 of the CEA.

6 Records Management (RM) program

6.1 General

The records management concepts, principles, methods and practices adopted by the organization shall demonstrate that an appropriate RM program is in place and is an integral part of the organization's usual and ordinary course of business.

The RM program shall support a records system consisting of appropriate records procedures and controls that complement business operating procedures. An organization shall

a) establish the RM program;

b) develop a RM policy, with definitions and assignment of responsibilities;

c) design RM procedures and related documentation;

d) select and implement technologies supporting the records system;

e) establish records protection measures, including audit trails and backup; and

f) establish a records quality assurance process.

6.2 Establishment of the program

6.2.1 Authorization

An organization shall authorize by a formal instrument (e.g. policy, directive, executive order, bylaw) the creation of a manual detailing its records system and setting out the policies, roles and responsibilities, and procedures for records creation, maintenance and disposition. The authorization shall reference the legislative authority and responsibilities of the organization with regard to the RM program, shall confirm that the RM program forms part of the organization's usual and ordinary course of business, and shall state that the RM program controls in an integrated way both electronic and hard-copy records. In addition to designating an individual or position as the appropriate signing officer or authority (i.e., RO), the authorization shall articulate the following:

a) legislative authority and responsibility of the organization to create a RM program;

b) purpose of the RM program;

c) extent of the RM program (i.e., ownership, custody, control, and applicability), and any exclusions;

d) means of implementation of the RM program (i.e., designation of responsibilities);

e) required RM procedures (i.e., records creation, management, use, destruction, and preservation); and

f) required quality assurance that certifies that all RM duties are appropriately fulfilled.

6.2.2 Responsibility

The role of the RO shall be clearly defined in the organization's formal authorization instrument (e.g., policy, directive) as responsible for implementing the RM program as an integral part of the organization's usual and ordinary course of business. The organization shall identify any other responsibilities to be assigned to the RO and other individuals or positions to ensure compliance with the RM program (e.g., an IT systems Security Officer (SO) responsible for ensuring IT system integrity).

6.2.2.1 Delegation of responsibility

An organization may implement a RM program or may delegate all or part of the program to an authorized third party (e.g. an external service provider). In any delegation, the roles and responsibilities of the authorized third party shall be clearly specified and documented to ensure that the trustworthiness of the electronic records is not compromised.

6.2.2.2 External service provider

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

6.2.2.3 Use of external service provider services

In the contract, the detailing of procedures, processes and practices shall cover any type of service, including facilities management and electronic records storage, conversion and migration, and security. The contract is intended to ensure that the external service provider complies with the organization's policy, procedures, processes and practices. The organization shall hold a copy of, or have access to, the external service provider's proof of compliance and the effectiveness and security of the service.

The organization shall not use an external service provider without ensuring that the external service provider signs a confidentiality and privacy protection agreement or is otherwise contractually bound to protect the organization from any breach of confidentiality or privacy.

6.2.2.4 Changes to the program

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

6.3 Policy

6.3.1 Requirement for a policy

An organization shall have a formal instrument (hereinafter "RM policy") stating that the management of electronic records is an integral part of its usual and ordinary course of business.

In some environments, it is useful to combine the RM program authorization and policy into one formal instrument.

6.3.2 Content of the policy

The RM policy shall contain statements to

a) identify the records and the records system covered under the formal instrument (i.e., policy or by-law), and any exclusions;

b) identify relevant RM and IT standards;

c) establish the position of RO having responsibility for the records system or give authoritative recognition from senior management to an existing position with the same responsibility;

d) require that the records system comply with the RM manual, the law, and national and industry standards so that the system will always produce and/or store records admissible as evidence;

e) grant the RO the responsibility to maintain and amend the RM manual with the support of IT staff so that it continuously reflects the exact state of the records system and can stand as evidence of the system's compliance with the law and this standard;

f) list the high-level requirements for records creation, management, use, destruction, and preservation;

g) ensure that IT staff works with the RO to integrate records management into the organization's usual and ordinary course of business, and to maintain that integration; and

h) identify the RO responsibilities with respect to records quality assurance and for monitoring compliance with the support of IT staff.

6.3.3 Compliance with the policy

Compliance with the policy requires the following:

a) authorization of the person (individual or position) responsible for obtaining and maintaining such compliance;

b) identification of the relevant legislation, directives and regulations that the organization shall comply with;

c) identification of any relevant national or international standards or part thereof that the organization shall comply with; and

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

The above documents shall be noted in the RM policy. Periodic audits shall be conducted to verify compliance.

6.4 Manual

6.4.1 General

The implementation of a RM program requires the use of a RM manual that consolidates all records related procedures to ensure consistency and completeness. The RM manual shall be consistent with the RM policy and any identified standards.

The RM manual shall describe the procedures for making, receiving, capturing, managing, using, protecting, destroying, and preserving records through their lifecycle. Changes to the RM procedures shall be authorized, documented, disseminated, and included in the manual.

The RM manual shall be kept up-to-date and accurately reflect the exact nature, functions, procedures and processes of the organization's records system, i.e., the way in which this system participates in and supports the usual and ordinary course of business, and the way in which the rapid change of technology impacts procedures and processes.

The RM manual shall specify the operation and use of the records system and include references to other relevant documentation (e.g., other procedure manuals, business procedures, IT system documentation) as appropriate. The RM manual shall have a formal review cycle to ensure ongoing alignment with other organizational requirements.

6.4.2 Records capture

6.4.2.1 General

Records may be generated by the organization or imported into its records system from an external source. The RM manual shall specify that documented control procedures shall exist for both types of capture, and quality assurance levels for accuracy and completeness of captured records shall be specified.

Where workflow systems are implemented, operational details and change-control procedures shall be documented in the RM manual. Such details should ensure that record integrity will not be compromised during a workflow process and records will not be lost.

The procedures used for non-textual records (e.g. audio, images, video and multimedia) shall be documented in the RM manual in the same manner as those for any other record forms.

The RM manual shall specify procedures enabling implementation of systematic version controls for all records. Responsibility and procedures for replacing stored records with new versions shall be documented in the system documentation. A record version control-procedure shall be established for all records.

A complete set of metadata including all evidentially relevant information on the identity of each record, the business rules associated with its capture, its logical structure, and complete entity and attribute definitions (see Annex B) shall be captured or created and maintained in the records system for as long as the record exists, sometimes longer. An organizational metadata profile shall be established for records.

6.4.2.2 Digitization

Any digitization process shall be carefully aligned to business needs and designed to create sufficiently high-quality digital substitutes of analogue records, with minimal loss of information, so that the digital substitute will serve ongoing business needs as well as unanticipated future requirements. The RM manual shall contain a listing of legacy and current analogue records approved by the organization for digitization, and document the legal and business rationales for authorized destruction of any source records. Re-digitization of born-digital records shall be avoided due to inherent losses in record quality and in business productivity.

The RM manual shall outline routine, authorized digitization procedures and processes, resulting in accurate and legible reproductions of source records without alterations to the content or appearance, along with appropriate metadata for the management and retrieval of the records. At minimum, quality controls shall be set at the document preparation stage, at scanning and indexing, and at the bulk upload stage. Quality assurance shall be conducted and certified by the organization, and source records shall not be subject to authorized destruction until all quality assurance procedures are completed, and all corrections and retakes are documented, approved, and submitted.

Where vendors provide digitization services, the vendor shall complete quality assurance as contracted, and provide a certification of assurance for all digitized records. Similarly, an organization's in-house scanning operators shall be trained to meet all quality assurance requirements and shall indicate completion of quality assurance activities through signatures or other modes of identification (e.g. stamps, marks, electronic identifiers).

Organizations shall be able to attest that the digital versions of the analogue records are complete and accurate, and thus capable of providing evidence of the activities in which the source records participated. These digital records shall be discoverable and available to those with the right to access them for as long as they are required.

6.4.3 Classification and indexing

Classification and indexing are key components of every RM program in that they allow for a logical organization of records, and for their identification, control, retrieval and disposition. All records should be classified in order to fix them into their documentary context, and indexed in order to facilitate their retrieval. With electronic records, these functions are implemented through metadata (see Annex B). It is required that the following be clearly outlined in the RM manual:

a) the specification of the classification methodology used (e.g. functional classification) and a representation of the classification system by means of a schema;

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

c) procedures for updating classification schema and index;

d) procedures for amending inaccurate classes, codes, or index terms;

e) procedures for implementing c) and d).

f) methods for tracking updated, deleted or destroyed status of classification codes and indexing terms; and

g) procedures for performing quality assurance of classification and indexing.

6.4.4 Records maintenance and use

The RO shall oversee and coordinate all the activities associated with ensuring the records in the records system remain authentic, available, and secure.

The RO shall maintain a record of the authority to retrieve, read, annotate, edit, transmit and delete records in the record system (i.e. access privileges), granted to officers and employees of the organization. The RO shall ensure that the nature of any action undertaken upon the records is documented, whether through additions of integrity metadata (see Annex B) or by compilations of reports, to provide an audit trail (see 6.5.5) of what has happened to the records since their creation. Such information is necessary when assessing the ongoing trustworthiness of the records in the system.

6.4.5 Records retention requirements

The time period for which records shall be retained shall be determined by authorized individuals or positions within an organization, including those responsible for the organizational functions that the records support, i.e., the legal adviser (to ensure compliance with legislation), the financial officer (to ensure compliance with financial requirements), and the RO (to ensure that retention and disposition decisions are based on sound records management and preservation principles and methods). Record retention requirements shall be documented in the organization’s Records Retention Schedule, which should be linked to the records classification schema. The assignment of the responsibility for identification of records retention requirements to authorized individuals or positions (e.g., the RO) shall be formally documented.

Retention periods are usually based on the value of the records and the organization’s need to access as well as evidentiary, risk management, legal and audit requirements. It is the responsibility of the organization’s RO to ensure that a proper appraisal of the records is conducted based on

a) how the records are used by the organization (internally and externally);

b) users’ needs for access to the records in the event of a disaster;

c) financial, legal, social, political, historical value of the records;

d) costs/benefit analysis of records retention;

e) impact on the organization if the records are destroyed; and

f) evidentiary capacity of the records in the event of litigation, audit or investigation.

After the value of each set (class or category) of records has been identified, then the RO shall document the length of time to retain the records, and how to transfer them to the designated custodian (for either a determined period of time or permanent retention), or how to destroy them after they are no longer required.

Whether an organization will need to keep the records for short or long periods or indefinitely, the organization shall ensure that the technological environment is able to support any such retention (e.g. fixed-date or event-based retention, or permanent retention). Furthermore, before any disposal decision (be it destruction or transfer) is implemented, it shall be reviewed by the RO, in case legal hold is required (see 5.4) or an event has occurred that involves a longer retention period.

The organization’s records management policy shall also define “transitory records” — records to which no retention requirement applies and which have no value in documenting or supporting the organization’s business.

6.4.6 Records disposition

6.4.6.1 General

Disposition refers to the action taken on records after the expiration of the records retention period: destruction, transfer, or preservation. Conducted in compliance with a Records Retention and Disposition Schedule, records disposition is regarded as an integral part of an organization's usual and ordinary course of business. The RM manual shall prescribe that all dispositions be documented. The RO shall be given the authority to suspend the destruction or transfer of records subject to legal hold (see 5.4), organizational or government review or audit.

6.4.6.2 Disposition process

The RM manual shall require that records disposition occur after the appropriate retention period has expired, disposition has been authorized, and any barrier to elimination has been removed. The organization shall be capable of submitting documentation of the disposition of its records when proof is warranted or required, based on business, legal or audit requirements. This documentation should identify the records disposed of using the associated metadata (e.g., the classification code, inclusive dates, office of primary responsibility), the organization who authorized the disposition, and the time of disposition. This record of disposition actions shall be kept permanently as proof by the organization.

The RM manual may require that metadata be retained after the records they relate to have been disposed of; the metadata should then record the event of disposition. If an electronic record is associated with more than one aggregation of records, it may be disposed of in the context of one aggregation and retained in the context of another; in this case the disposition is carried out by deleting from the record metadata associated with the set of records that is disposed of.

6.4.6.3 Destruction of electronic records

System transaction logs, audit trails and other appropriate records of destruction and amendment activities may need to be retained permanently. It may be required to destroy a specific record from a records system because of legal or administrative requirements, particularly in accordance with privacy regulations or other legislation. The RM manual shall allow the records system to destroy, amend or correct records using an editable process. For destroyed records, the system procedures shall ensure that both the record and the locator are destroyed. The destruction of electronic records needs to be completed in such a way that the confidentiality of the records is preserved, and personal information is not disclosed.

6.4.6.4 Transfer of electronic records to another entity

The RM manual shall require that records transferred to and accepted into custody by a designated custodian (e.g., an archives) appear in the documentation of both the transferring and the receiving body. It may also require the identification of the hardware and software that generated the records, and the program documentation that describes the format, file codes, file layout and other technical details about the records system in which the records resided.

6.4.6.5 Records preservation

The RM manual shall emphasize that, in the digital environment, preservation begins with the controlled creation and maintenance of records in preservable file formats, with the essential identity and recordkeeping metadata (see Annex B) required to demonstrate that a record was made or received or stored in the usual and ordinary course of business, is authentic, and has been properly maintained in the records system without unauthorized modifications.

An organization's records system shall have the ability to permanently retain those records whose value to the creator is enduring. Records created by organizations may have enduring value and qualify for permanent preservation, and shall be safeguarded against software obsolescence.

6.4.6.5.1 Records conversion and migration

The RM manual shall provide guidance on conversion and migration. Records conversion and migration are methods used to overcome software obsolescence, which results in the inaccessibility of electronic records over time. There are two kinds of digital record obsolescence: file format obsolescence, where available software applications can no longer open or view the contents of a digital record; and system obsolescence, when a system or application is no longer supported (in some cases due to hardware obsolescence) and the records cannot be retrieved, opened, or viewed. File format obsolescence shall be addressed by file conversion, that is, by moving a record from one file format to another (the native application or source file should also be maintained). System obsolescence shall be addressed either by migrating digital files to a new system or application (often leveraging system virtualization), or, in rare cases, keeping the old hardware or buying specialized software to access obsolete media.

Conversion and migration always involve risk, and, before undertaking them, the organization shall identify the required functionalities of the old format and those that have to be maintained in the new format and system, and document such decisions, as different software may render the same record in different ways. Regardless of the preservation format that is chosen, both conversion and migration shall be integrated in a well-documented business process that is part of the regular operation of the records system.

Organizations shall have a conversion and migration policy, and the RM manual shall outline detailed procedures ensuring that records' structure, content, identity and recordkeeping metadata (see Annex B), and, in the case of email, attachments, links, proof of delivery, distribution lists, and relationship to other records of the organization within and outside the organization are protected and preserved. A checksum enabling the verification that there have been no errors in conversion or migration should be required for each file.

6.4.6.5.2 Preservation formats

The RM manual shall identify the organization's preferred formats for preservation by type of record. A variety of resources exists to aid organizations in selecting the proper preservation formats for their records and carrying out the conversion. The decision on the preservation format shall be based on how much change can be introduced before the record representation becomes too degraded to serve as a reliable copy of the record in its native format in a legal proceeding (see Annex C).

6.4.7 Quality assurance

In essence, a records management program is a quality assurance program designed to support the creation, management, use, destruction, and preservation of trustworthy records that provide evidence of an organization's activities in the usual and ordinary course of business. While the records management policy and manual documents the controls that the organization has put in place to support record and system integrity, quality assurance is required to ensure that the organization's records management program is compliant and meets legislative, administrative, operational, and technical requirements on an on-going basis and that any fraud or abuse is either avoided or uncovered and addressed at the earliest juncture.

Quality assurance means that the organization defines the appropriate level of service, and ensures staff understand their roles and responsibilities and are trained to provide this level of service. To this end, the RO shall implement appropriate quality assurance processes, including but not limited to performance and compliance monitoring, self-assessment and external audits, and incident handling, and record and certify that all RM duties are fulfilled. The RO shall immediately report all significant issues to the senior executive in charge of the program who shall respond as required and direct and/or approve necessary RM program adjustments.

6.5 IT system management guide

6.5.1 General

All significant details of the logical and physical architecture of the IT system keeping the records shall be fully documented in the IT system management guide, including the responsibilities and the relationships between IT system management, the RM program, and the conduct of the organization's business. The IT system management guide shall be structured so that the integrity of the system can be demonstrated for any point in time. The documentation required for the IT system shall include the following:

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

b) description of operating systems and application software, including record formats;

c) description of IT security protections such as firewalls, system backups, and disaster recovery;

d) description of system integrity verification procedures, including event scheduling and accountabilities, for monitoring and maintaining systems and data integrity and for taking preventive and corrective action where required;

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

f) documentation of changes to the system, including all responsible individuals or positions and a full account of the processes and activities undertaken to affect the change; and

g) procedures to control the use of system maintenance hardware and software that can bypass system access controls, and necessary authorizations for their use.

The manager responsible for the IT system shall ensure that the IT system management guide is kept up to date.

6.5.2 Backup and system recovery

Effective procedures for the backup of electronic records and all associated information (e.g., index files and audit trails) as well as those for system recovery shall be included in the IT system management guide. Only authorized individuals shall be allowed to enable or disable the backup and recovery functions.

The IT system management guide shall require that the storage media be tested to prove that no recorded information or metadata have been lost or overwritten, and that backups be tested at predetermined intervals for accuracy and integrity.

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. It is prudent to have several simultaneous backup copies of recorded information and application programs and to maintain one of these at another location. The IT system management guide 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 electronic records, the differences shall be documented.

The IT system management guide shall require that, where backup data files are used to recover from a system failure, procedures shall be documented to ensure that data file integrity has not been compromised. It shall also require that backup procedures and details about transfers shall be retained for as long as the referring records are required.

The technological aspects of backup and system recovery shall be covered by the IT system management guide. Mirroring and redundancy can substitute backup for system recovery in case of a disaster.

Backups are a product of the security function of an organization and should be regularly disposed of on a rotational basis according to an explicitly defined term.

6.5.3 Security and protection

6.5.3.1 IT security policy and procedures

An organization shall have an IT security policy specifying the levels of access to the records system (i.e., the whole of an organization's records and associated records management and preservation systems), as well as the levels of protection applied to the IT system (i.e., the whole of an organization's computers, software, and devices used to process and transform information).

Procedures shall be implemented in accordance with the organization's IT security policy. These procedures shall include a system-wide definition of user authentication and permission controls, privileged users, and notification of, and protection against, unauthorized access as well as guidelines on access and changes in personnel with access. Security screening of individuals working for the organization shall be in accordance with the information's level of sensitivity. The accommodation and operating environment for the storage, transportation and maintenance of storage media shall be in accordance with relevant national or international standards.

6.5.3.2 Encryption and secure electronic signatures

Where there is a requirement for the safeguarding of recorded information, encryption shall be used to improve the security and ensure the integrity of recorded information during transmission and storage.

Where secure 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 individuals.

6.5.3.3 Self-modifying electronic records

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 fixed. Each time the file is retrieved, it may appear to be different although the user has not changed the stored file.

Within an evidentiary requirements context, this is directly related to "the usual and ordinary course of business," which includes registration of the fact that the records of an organization change. It is necessary to differentiate among the types of changes, whether they affect the content of the record, the metadata, or the documentary form. To ensure that an electronic record can be used as evidence in a legal proceeding, organizations shall prevent any form of automatic modification to the approved version so that authentic copies can be provided.

6.5.3.4 Date and time stamps

The regular checking of computer system clocks for accuracy concerning date and time keeping shall be documented. Date-keeping and time-keeping involve the ability to detect and correct errors. All actions taken concerning error correction or resetting of system clocks on all computer systems and devices shall be documented.

An organization shall identify the individuals who are authorized to access and modify system clocks, and ensure that appropriate access control measures are established.

6.5.4 Records transmission

Organizations shall ensure that there is interoperability among the technologies they use and with the technologies used by any other organizations with whom they interact in the usual and ordinary course of business. When records are being transmitted between computer systems, applications, or storage media, records integrity shall be regularly checked through a verification procedure.

6.5.5 Audit trail

6.5.5.1 General

Audit data represents the history of each record and the associated metadata. Audit data is the definitive proof that certain events and transactions occurred. As such, the capture of audit data shall always be an ongoing process and audit data shall always be protected from alteration and loss. Audit data is collected into the audit trail.

Audit trails shall contain sufficient and necessary audit data to provide evidence of the authenticity of the records made by the organization and of the integrity of any received records from the moment of receipt. The audit trail of an IT system shall consist of system-generated and operator-generated logs containing data about capture of and changes to (e.g., modification, deletion, access) the records stored on the system. The integrity of the audit trail is important to satisfy the best evidence rule, as required by the electronic records provisions of the Evidence Acts, and for establishing the weight to be given to records (i.e., their probative value and persuasiveness as reliable records).

Procedures for audit trails shall be documented in the IT system management guide.

6.5.5.2 Management of audit trail records

The audit trail logs shall be subject to internal records management procedures similar to those for other essential records of the organization and shall be included as a specific document type in the IT system management guide. Audit trail data kept within the records system shall be made unalterable in the secure environment. Secure backup copies of the audit trail shall be kept.

6.5.5.3 Content of the audit trail

The organization shall establish the content of the audit trail.

The following are minimum content requirements:

a) identification of the recorded information to which the action was applied (including unique identifiers);

b) individual or position responsible for initiating and carrying out the action; and

c) date and time of events such as:

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

   ii) creation of new electronic record versions;

   iii) creation, amendment and deletion of metadata;

   iv) changes in access authorization for records or data;

   v) changes in retention and disposition requirements;

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

   vii) modification, destruction or transfer of records or data.

6.5.5.4 Audit trail creation

Audit trail data shall be generated automatically by the IT system. If it does not happen, the procedures for generating audit trail data shall be documented in the IT system management guide. These procedures shall apply to the organization and any contracted external service providers.

For records selected for permanent preservation, the designated preserver shall have access to audit trail data in order to verify the authenticity of the records.

6.5.5.5 Access

Access procedures and authorizations to audit trail data shall be documented in the IT system management guide.

6.5.5.6 Audit trail of conversion and migration

If records are moved between storage devices as part of a conversion or migration process, details of the process shall be stored in the audit trail. Procedures for migration or conversion shall include methods for proving that any related metadata are also migrated or converted and be documented in the IT system management guide. Where records have been converted from one file format to another, details of the conversion shall be stored in the audit trail log.

6.5.5.7 Workflow

Where workflow systems exist, the IT system management guide shall define at which points in the workflow audit trail data shall be generated and kept in the IT system. In a typical workflow system, audit trail data are generated at each step in the workflow.

The audit trail data to be generated and kept may change as the workflow processes are changed.

The IT system shall permit an authorized individual to select the audit trail points for which audit trail data are generated.

6.5.5.8 Verification

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

7 New technologies

Increasingly, organizations are creating, managing, and using records in a variety of environments, services, and devices over the Internet. The benefits and risks of adopting these shall be established through a process of risk assessment.

7.1 Risk assessment

Prior to commencing the adoption of a new technology, the organization may:

a) establish a Risk Assessment team (i.e. risk manager, IT enterprise architect, IT network analyst, legal expert, SO, and RO) to consider the new technology and make recommendations on adoption;

b) reference the organization’s existing risk management framework (i.e. policy, procedures, and guidelines);

c) identify stakeholders and determine participation venues;

d) identify, assess and mitigate threats and risks associated with the new technology;

e) ensure reporting mechanisms to senior management are in place, and that senior management has made their determination prior to the commencement of new technology adoption;

f) develop policy and documented procedures for the new technology (including updating the RM manual and IT system management guide);

g) develop a decision-making process for current and future proposals relating to the new technology; and

h) communicate policy and procedures for the new technology to staff.

The risk assessment provides a tool to identify, classify and weigh the risks and provide information to use in developing risk mitigation strategies and policies. The complex legal implications of new technologies shall be carefully considered using a multi-disciplinary approach (e.g. legal, security, privacy, IT, risk management, etc.) that takes the organization's existing infrastructure and risk tolerance into account.

7.2 Cloud computing

7.2.1 Jurisdictional location

When using cloud computing, an organization shall discover under which jurisdiction its data/records are kept. It is common for a Cloud Service Provider (CSP) to have data centres in several countries. Furthermore, as digital materials continuously move from a server to another for space availability and the security ensured by geographical dispersion, it is practically impossible to establish where they are at any given time. Canada does not allow for the recorded information held by public organizations regarding its citizens, as well as and any data transmission and backup routes, to reside outside its boundaries, and it shall be the responsibility of the public organizations to comply with this rule. Thus, jurisdiction is the first fact public organizations shall ascertain before considering a cloud computing solution; private organizations should also consider jurisdictional issues.

7.2.2 Privacy

Privacy is a second major issue with cloud computing. Even when recorded information is physically kept within the boundaries of Canada, online access means it may be accessible from anywhere, as well as hacked, tampered with, or included in different contexts. Additionally, there is no guarantee that records scheduled for destruction will in fact be destroyed at all locations where they exist due to redundancy and backups. In many cases, access links are eliminated but the material is not destroyed. Given the Canadian legal requirements around personal information, these access issues and involuntary permanence of records present significant liabilities associated with cloud computing.

Organizations shall ensure through contractual agreement with the CSP that they will be immediately notified in the event of any access breach and that their retention and disposition requirements and procedures shall be implemented by demonstrating that the records are protected, preserved and destroyed as directed. The agreement with the provider shall ensure that if litigation, audit, or government investigations occur, or are expected to occur, regularly scheduled destructions of related records are immediately suspended and that the assigned retention period is resumed once the hold is no longer required.

Organizations shall include in the agreement with their CSP provisions related to the storage of and responsibility for records of terminated employees.

7.2.3 Admissibility rules

When cloud computing is used, the records entrusted to such environment shall still satisfy admissibility rules. The RO, with the support of IT, shall develop a means of authenticating records entrusted to the cloud and identifying which instance of the same record constitutes the organization's official record. The records creation, maintenance and use in the cloud environment shall be documented (see Annex D).

7.2.4 Records system integration

Considering the fact that every organization has records to which it cannot afford to risk unauthorized access or loss of access (e.g., sensitive records), organizations choosing cloud computing for those records shall maintain a hybrid records system, with such records remaining in the in-house infrastructure. The organization shall ensure record program requirements are met irrespective of whether records are stored by one or more cloud providers or in-house.

7.3 Social media

When an organization uses social media, there are issues from an evidentiary point of view, notably

a) the identification of records;

b) the determination of their author, and owner (necessary in order to establish who has a duty to identify, capture and manage the record);

c) the definition of their context (and therefore the ability to determine whether they are generated in the usual and ordinary course of business);

d) the assessment of their reliability, accuracy and authenticity; and

e) the identification of a chain of custody (particularly if individuals upload business records to their own social media pages or those of others).

Organizations shall develop a social media policy which shall define when a posting is considered to be a record. They shall define the process through which records are captured, including the creation of an authentic copy with identity metadata that clearly indicates the context of the posting, the responsibility for it, and any related actions.

Existing records of the organization that are posted on social media as links shall be maintained by the organization in accordance with the existing classification, index, and retention and disposition schedule, taking into consideration, however, that social media providers retain such records indefinitely.

When the possibility of litigation arises or is anticipated, it may be necessary to take additional snapshots or images of relevant material, since social media sites can be shut down, accounts or memberships terminated, and content deleted (see Annex E).

7.4 Mobile devices

Organizations may allow employees to bring and use their personally owned devices in the execution of their duties when it would appear that the benefits outweigh the risks. BYOD/BYOC introduces a number of challenges related to database and software licensing, security, privacy, intellectual property, and employment law due to the “borderless” nature of device use (see Annex F).

Following a risk assessment process, the organization shall provide a clearly articulated, strictly enforceable policy. The policy shall explicitly state whether it supports BYOD (by either managing all records created on personal devices or only the records created on such devices by a segment of the organization), allows but does not support it (i.e. each employee is responsible for managing the organization’s records in the device or transfer them to the organization recordkeeping system), or does not allow it. In the latter case, it should state whether it enables COBO (Corporate Owned Business Only) devices or COPE (Corporate Owned Personally Enabled) devices, or whether it allows each employee to choose among the three options. In each case, the policy should include details such as: type of devices used, employer-employee cost-sharing, access rights, support arrangements, tracking and monitoring, remote wiping, activity prohibitions, preclusion of use by anyone other than the employee, and reciprocal obligations at the termination of employment.

Procedures for managing records using BYOD/BYOC shall be incorporated within the RM manual; procedures for managing devices shall be incorporated within the IT system management guide.

Annex A
(informative)

Sources for this standard

A.1 Introduction

This annex sets out the sources that have been considered for this standard.

CAN/CGSB-72.34 is based on the law of evidence for the admission of documents commonly referred to as documentary evidence. It focuses on those documents that the Canada Evidence Act regards as an exception to the hearsay rule, that is, business records. The law on this question is a mix of common law (laws developed through case decisions by judges, not enacted by legislative bodies) 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 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.

A.2 Sources

The sources for this standard include:

a) Canadian legal requirements, including legislation and pursuant regulations (federal, provincial, territorial);

b) Information, communication, and technology (ICT) requirements and standards;

c) Business operation requirements and best practices (and related standards); and

d) 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 is drawn from well-known Canadian professional and industry associations in the areas of records, information, and image management; legal and financial services; and accounting and auditing. The experts represent both user and supplier perspectives, ensuring a balanced approach.

Annex B
(informative)

Metadata

B.1 The production, management, disposition and preservation of metadata should be formally authorized by the organization in the RM manual.

B.1.1 The RM manual should identify that metadata:

a) is information about records, regardless of medium, that is used to identify, describe, manage, authenticate, and access those records;

b) is kept and used in the usual and ordinary course of business by the records creator and is discoverable;

c) is produced at the time of records creation (i.e., when a record is made or received or stored to an aggregation of records);

d) is an integral part of a record. Additional metadata accumulates over the record's lifecycle and its production and management forms an integral part of the records system;

e) allows users to understand and interpret the record; and

f) supports the assessment of its trustworthiness, that is, its reliability, accuracy and authenticity as evidence.

B.1.2 Metadata may be classified according to the time of its accumulation and its purpose. Metadata generated at the time of creation to identify the record is *identity metadata.* It may include:

a) Time metadata – attributes specifying the date a record is made or received or stored to an aggregation of records;

b) Persons metadata – attributes specifying the names of the record author(s), addressee(s), and other recipients, and of the handling office, if applicable;

c) Form metadata – attributes specifying the documentary form of the record (e.g. letter, memorandum) and the intellectual form of the record (e.g. contract, sentence, patent, application);

d) Technical metadata – attributes specifying the format and other technological characteristics of the record;

e) Naming metadata – attributes stating the name of the record, its subject matter, or the action it embodies;

f) Relationship metadata – attributes specifying the relationships of the record to other records (e.g. registry number, classification code, identification number); and

g) Authentication metadata – attributes specifying the method of authentication of the record if applicable (e.g. digital seal, digital signature, encryption).

B.1.3 Identity metadata, being an integral part of the record at creation, should be maintained with the record for as long as the record exists, otherwise the record will lose its integrity.

B.1.4 Metadata added throughout the record lifecycle in order either to attest to technical or formal changes, additions, movement of location or of responsibility for the record, or to enable implementation of records management procedures and processes, including access and retrieval, access restrictions, retention and disposition, is recordkeeping metadata and can be categorized as follows:

a) Descriptive metadata – attributes used to find and interpret the record; and

b) Administrative metadata – attributes used to manage the record, which may include:

   i) Technical metadata – attributes providing information about the technical context of the record, the migration to a new system, and methods of disposition;

   ii) Rights metadata – attributes describing rights and obligations adhering to the record, including ownership, copyright and other intellectual property rights, usage and security restrictions;

   iii) Preservation metadata – attributes describing activities carried out to preserve the record over time and across technological change, such as conversion and reproduction for redundancy;

   iv) Structural metadata – attributes documenting the structural relationships between or within digital records (e.g. the linkage between pages in a website);

   v) Use metadata – attributes about or from the users of the resource (e.g., social tags, access logs, user search logs).

B.1.5 Recordkeeping metadata is not part of the identity of the record, but being generated in the course of its maintenance and use, reveals the actions in which the record has participated as well as the usual and ordinary course of business. Metadata can be destroyed when superseded but only if such action is part of the usual and ordinary way in which the creator manages its records. The organization should keep in mind that metadata may include personal information, and therefore be subject to privacy law.

Annex C
(informative)

Preservation formats

The following discussion is illustrative and does not have the purpose of recommending a specific format—as the standard is technology agnostic—but is meant to show the considerations that need to be made when selecting a preservation format (e.g. an open format which is widely recognized).

In terms of textual records, there is one file format designed specifically for the long-term preservation of records. The Portable Document Format (PDF), ISO 32000-1: 2008, is a file format for delivering page-based documents in a platform independent manner, preserving the appearance of the document when viewed across multiple architectures. If, however, the accurate display of fonts is an evidentiary requirement, format PDF/A, ISO 19005-1: 2005 is preferred. Although it does not allow audio/video content, JavaScript, compression, and encryption, it requires that all fonts be embedded and uses Adobe's Extensible Metadata Platform (XMP) metadata rules with the ability to supply new metadata schema if needed. PDF/A-2, ISO 19005-2:2011 and ISO 32000-1 increased accessibility, included improvements for smaller file sizes, permitted the use of JPEG2000 image compression, and allowed attachment of other PDF/A files. PDF/A-3, ISO 19005-3:2012, has the same functionalities as PDF/A-2 but, in addition to other PDF/A files, can embed any kind of data stream. Document viewers designed to work with the specification will display the record content just as with PDF/A-2, but can have an additional recommended functionality where, at the user's request, the embedded data can be extracted from the PDF and used/opened in any desired manner.

From the perspective of records conversion and migration of documents, either to address issues of obsolescence or simply to improve readability or usability across platforms, it would appear that the PDF/A-3 could support evidentiary requirements from both a business records and a best evidence perspective. While the static visual elements of the main display document present the record content with fixity, a larger contextual metadata set (or sets) could be stored in the 'dumb' data sections to ensure authenticity. Any concern about best evidence or integrity can be addressed with the embedding of the original bitstream of the source record itself.

Annex D
(informative)

Cloud computing

D.1 Cloud computing is the use of a broad range of infrastructures and services distributed across a network (typically the Internet), scalable on demand (whereby capabilities can be elastically provisioned and released), and designed to support storage and management of high volumes of digital materials. Essential characteristics of cloud computing are: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service.

The most common service models are: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Cloud Services Providers (CSP) leverage a number of deployment models including: private cloud, community cloud, public cloud, and hybrid cloud. It is important not to confuse cloud computing with the use of the Internet for storing an organization's own records on line in a space controlled by the organization.

The standard of trustworthiness for the use of cloud computing offered by an external CSP is that of the ordinary marketplace: *caveat emptor,* or buyer beware. Organizations using cloud computing provided by external CSPs put themselves in a relationship of voluntary vulnerability, dependence and reliance, based on risk assessment; every organization should consider the benefits of using cloud computing in relation to the risks of doing so.

D.1.1 Cloud computing offers several benefits:

a) Cost reduction – the most evident benefit as organizations do not have to own the network hardware/software, and can avoid significant upfront costs. In addition, there may be reduced information technology personnel costs; reduced energy costs; no cost for technology upgrades as the shared-tenant system allows pooling of resources to get more for less; and contained costs, as the organization pays only for services used.

b) Scalability – service provision is flexible and can be increased or reduced as required.

c) Availability – services are available on demand, at any time, and at any place, given network access.

d) Security – Cloud Service Providers (CSPs) may leverage critical mass to offer more complex and expensive technologies and centralized control than would be available at any single organization.

e) Collaboration – users in the same or different geographic locations can consistently access and share materials that are continually updated and made available from a central source.

D.1.2 These same benefits bring risk. Organizations should conduct a risk assessment with regard to the adoption of cloud computing in consideration of a number of factors.

a) Cost – cloud computing costs remain significant. The transfer of existing information assets, establishment of new business processes, implementation of controls and encryption, and per-request fees may be higher than projected. Organizations may experience high variability of costs based on changes in patterns of use, and unexpected costs such as licensing fee increases.

b) Scalability – organizations may face difficulties in tracking and estimating their service needs.

c) Availability – organizations are dependent on the CSP to provide service and business continuity.

d) Reliability – CSP may lose information assets through faulty processing or backup procedures. A CSP may be acquired, go bankrupt, or otherwise disappear with insufficient notice.

e) Portability and interoperability – organizations may face difficulties in transferring digital assets between providers or services.

f) Security – unauthorized access by CSPs, sub-contractors, hackers, and internal threats present the most significant security risks to digital assets held or in transit, along with inadequate access management. Multi-tenancy presents the possibility that digital assets may be co-mingled with those of another organization. Application Program Interfaces (APIs) may lack necessary security features. Security controls may be under-monitored or ignored.

g) Terms of service – organizations' expectations may not be met in a standard contract with a CSP, particularly with respect to production and ownership of metadata, privacy requirements, and compliance and audit needs.

h) Controls – organizations may experience difficulties in proving the trustworthiness of their recordkeeping system and of a specific record required as evidence. Significant controls are required to prove the authenticity (i.e. identity and integrity) of records, and these are less available to organizations through cloud computing.

i) Transparency – organizations may find after-the-fact that CSP do not provide sufficient information or access to support requirements for records as evidence.

D.2 As the processes of records creation, maintenance and use, and the legitimate chain of custody might not be as easily demonstrated in the cloud compared to those for records kept in-house, the nature of business records in the cloud can be more easily challenged by the fact that materials in the cloud can be hacked and tampered with. This also implies that records in the cloud cannot have forensic integrity, in that their keeping, processing and preservation are not repeatable, verifiable, or objective, as prescribed by digital forensics authentication processes, therefore they cannot be used as evidence. Neither can records in the cloud have duplication integrity (i.e., the process of creating a duplicate of a record does not modify it either intentionally or accidentally and the duplicate is an exact bit copy of the original). This type of integrity is extremely important to preservation because we can only preserve digital records by reproducing them, so transparency about the reproduction and migration processes is essential to trusting records. Either the method used to gather and analyse or acquire and preserve digital records should not change the digital entities, or, if it does, the changes should be identifiable. Admissibility of records held in a cloud environment is possible if the contract with the CSP includes clauses that allow access to the identity and recordkeeping metadata (see Annex C) and the ability to verify the integrity of the system.

Annex E
(informative)

Social media

Social media are applications and services designed to facilitate collaboration through creation and exchange of user-generated content. The term includes: blogs/microblogs, wikis, RSS, multimedia sharing, social bookmarking/ tagging, social networking services, mashups, virtual worlds, and collaborative editing tools. Social media applications use the web as a platform, share user generated content, often gathered through crowdsourcing, and build networks based on an architecture of participation and openness. Content generated by social media applications is often offered as evidence but can be difficult to capture, preserve, and authenticate.

Like cloud computing, social media present many challenges, notably privacy breaches, breach of confidentiality, defamation, copyright and trademark infringement, improper personal use (vs. acceptable use by the organization), human rights violations (discriminatory posts), workplace grievance (bullying and harassment in the workplace), and complying with court orders (not posting names from court cases under publication ban).

Regardless, governments use social media to provide customer service, access to information, notice of emergencies, and offer the opportunity for community involvement. In doing so, they cause the creation of public records, in particular when the public is engaged in decision-making and policy consultation, but also when public employees collaborate through means like the GCpedia (Government of Canada wikipedia). Social media applications most commonly used by governments currently include Facebook, Twitter and You Tube.

Organizations of all kinds use social media similarly to governments but more intensely for public relations and to carry out transactions, thus the electronic records they create in such processes are of specific concern when it comes to their use as evidence.

The primary characteristic of the records generated on social media is their apparent ephemerality and effective persistence. On the one hand, the dynamic nature of these sites makes it difficult to retrieve the records when needed, and on the other hand, the lack of control by the user does not guarantee records deletion when desired or required.

Another key characteristic of social media records is the lack of a stable context and the existence of multiple contexts, which may imbue the records with different meanings. Is the context of a tweet, for example, the page on which the tweet appears, or the previous and subsequent tweets of the same author? Is it the event to which it refers or the chronological time period of the posting?

Furthermore, a) social media platforms facilitate the movement of material from one circle of people to another, crossing public-private boundaries; b) contributions attributed or linked to social media accounts of people now deceased, or programs, committees, or agencies no longer in existence; c) ad hoc dynamic groups of employees collectively create bodies of interlinked material related to a work project or common interest, putting into question ownership and authorship; and d) the practice of reuse becomes often *remix*, a practice which results in derivative works that substantively change the intent and context of the appropriated material. New social norms are emerging through successive cycles of use, reuse, modification, repurposing, and take-down notices.

Annex F

(informative)

Mobile devices

BYOD is the acronym for “Bring Your Own Device” which is the emerging practice of employees of an organization to use their own laptops, tablets, netbooks, smartphones, or other mobile devices for work purposes. This practice is having and will continue to have significant impact over Information Technology security in the next few years.

BYOC is the acronym for “Bring Your Own Cloud” which is the emerging practice of employees to use public or private third-party cloud services to store their organization’s records. BYOC and BYOD are inextricably linked because, when an organization’s records are stored on mobile personal devices, they need to be accessed through the internet.

This global trend is called Consumerization of IT – COITT. Consumerization of IT is driven by employees who buy their own devices to carry out their organization’s work, use their own personal online service accounts, install their own applications and then connect to the corporate network with the device, often without the organization’s knowledge or approval.

BYOD and BYOC raise significant concerns, similar to those raised by cloud computing and social media: who owns the records? Who has access to them? Can the employee compartmentalize the records used for work so the organization can access them and the employee can protect his/her private information on the device? Does the data on the device meet the legal definition of “record”? Is it accessible for use? Are records on the device admissible in a legal proceeding as documentary evidence or real evidence? Can the organization be protected from theft or loss of the device, security breaches, defamation by the device owner, privacy breaches? How can the organization, following the lifecycle of the record, access, use, secure and preserve business information on the user’s device?

Organizations employ complex decision-making processes to secure their systems and sensitive information and to maintain reasonable and legally defensible security. They invest in technical, administrative and physical controls reflected in written security policies that they determine are sufficient to reduce security risks to an acceptable level.

Organizations will find it difficult to mitigate security risks when they do not control compliance with their own security protocols. Organizations should require security encryption of all sensitive information on organization-owned computer devices. It could be difficult to implement those standards on an employee’s mobile device. If the employee’s personal device is hacked or stolen and the unencrypted information accessed, the organization’s Mobile Device Security will likely be the first area to be scrutinized.

At the same time organizations should examine both the benefits and risks of BYOD/BYOC. Some organizations have already accepted these practices based on such an assessment.

Perceived benefits of BYOD:

a) Cost reduction – reduced or no investment in mobile or other hardware devices by organizations to equip their employees to perform daily functions.

b) Improved productivity – employees tend to spend more time using their devices, which are accessible to them around the clock. The possibility exists that productivity will increase because of such accessibility.

c) Efficiency – it is highly likely that employee devices are more up to date than organisation owned devices. This may lead to greater efficiency.

However, BYOD poses significant challenges concerning incident response and investigations impacting the reliability, accuracy and authenticity of the records, as well as employees’ privacy and organizations’ confidentiality and security. If there is a matter that needs to be investigated it may be difficult to actually obtain access to or possession of the device. This is especially true when the employee is the subject of an investigation. If the collection of documentary evidence contained in personal devices and its preservation is necessary, the inability to access and take custody of a physical device can be extremely detrimental. If an organization is not able to hold and protect the records that may constitute evidence in litigation, it could face court sanctions.

Many organizations are moving towards expanding the range of tools they use beyond smartphones and tablets and to embrace BYOD for PCs as well as Ultrabooks and mini PC's with a smaller footprint. It is likely that employers will discover new uses for emerging devices not initially understood by IT planners, a case in point being the iPad. More risk tolerant organizations may adopt a "try it and learn from it" approach to testing the advantages of using new devices.

The trend will not stop with BYOPC and BYOC, but "Bring your own IT" is imminent. These new tools will quickly encourage employees to bring their own applications, systems and possibly social networks into their organization.

While the opportunities are undeniable, it is expected that emerging events will force the late adopters to be conservative. These events could take the form of news of significant data leakage through employee-owned devices and concerns by employees and unions about the implications of having access all the time, anywhere — does this mean the employee is required to respond whenever/wherever? Employees' personal data and even individual locations could be visible to employers and this would impinge upon their privacy.

Early adopting organizations wishing to "force" employees into "BYOD" may face opposition where employees may see it as a move to cut costs at their expense. However, the hidden costs of shifting from an efficient IT support to employee's self-support may erode whatever savings can be derived from the BYOD practice. The issue will remain at the forefront for IT planners for some time even with evolving "iron-clad" BYOD policies.

Organizations should undertake extensive risk assessments in consideration of BYOD, focusing on the following:

a) Security – the probability of unauthorized access to sensitive information by both internal and external parties is high, so security should be high.

b) Redundancy – the likelihood that critical information be stored only on these devices, instead of on the organization's secured servers, requires that multiple copies of records be kept, in case a device is lost, destroyed or inaccessible at a critical time.

c) Auditability – organizations that process or handle confidential assets are frequently audited or require auditing of their security systems and processes. It would be difficult to acquire the requisite security clearances in a BYOD environment, because auditing of records kept in personal devices might constitute a breach of an employee's privacy, making it impossible to carry out comprehensive audits. This requires explicit procedures.

d) Data ownership – in a BYOD environment ownership of the records may become an issue and this will require a clear identification of what records residing in a personal device are legitimately owned by the organization.

e) Chain of custody – organizations will lose control over the records that are stored on employee devices, thus they need to regulate how those records are made or received or stored, how they can be used by other employees, how are copies made and controlled, and how they are transferred to the organization's servers to be controlled by the organization's RM procedures, like classification and retention and disposition, and to become integrated in the records system.

f) Management information – organizations will not have the immediate and continuing availability of the records required to make key management decisions, thus it shall be established which records need to be transferred or copied from the personal device on a tight timeline, or which records should be available on the organization's cloud at all material times.

g) Retention and legal hold – constant verification that the records identified for long term retention are protected is required, and so is the capability of establishing a legal hold on the records in the personal device as soon as required.

h) Disposition of information asset – often employees are not careful with the deletion of the records that need to be disposed of. It is essential to establish how records on personal devices will be securely destroyed without possibility of recovery according to the organization's retention and disposition schedule.

i) Data integrity – it is highly improbable that record integrity can be maintained or verified in a BYOD environment and this is the primary reason why strict procedures about transfer of the records to the organization's server or cloud environment are necessary.

j) Employee termination – when employees are let go or leave an organization, it is almost certain that records stored on the employee's device will be either deliberately or mistakenly taken by the employee, thus the organization needs a clear procedure to prevent as far as possible such an event.

k) Revenue loss – organizations stand to lose revenue when they do not possess all the records required to "bill" clients. There is also the possibility that employees use records stored on their device to potentially generate revenue for themselves. Regulations need to ensure that such events do not happen.

Two additional steps that can be taken to reduce the risks associated with BYOD and BYOC are the deployment of a Mobile Device Management (MDM) or Enterprise Mobility Management (EMM) solution and the use of a thin client – where an application accesses information that is processed and stored on an organization's servers.

Valid alternatives to BOYD are COBO (Corporate-Owned, Business Only), where organizations own the devices used by the employees and do not allow personal use of such devices, and COPE (Corporate-Owned, Personally Enabled), where employees are provided with devices that are owned by the organization but configured to allow the employees to use them for personal activities. It is possible for an organization to use a mix of strategies, depending on how structured and uniform it is. If parts of an organization have unique requirements or specific security profiles, the organization might want to support several solutions at the same time rather than selecting a single solution.

Bibliography

[1] American National Standards Institute (ANSI). ANSI/ARMA 18-2011 *Implications of Web-based, Collaborative Technologies in Records Management.* Available from: IHS Markit. www.global.ihs.com/

[2] American National Standards Institute (ANSI). ANSI/ARMA 19-2012 *Policy Design for Managing Electronic Messages.* Available from: IHS Markit. www.global.ihs.com/

[3] ARMA International. TR 24-2013, *Best Practices for Managing Electronic Messages.* Available from: IHS Markit. www.global.ihs.com/

[4] ARMA International. *Guideline for Outsourcing Records Storage to the Cloud* (2010). Available from: IHS Markit. www.global.ihs.com/

[5] Canadian General Standards Board (CGSB). CAN/CGSB-72.11, *Microfilm and electronic images as documentary evidence.* Available from: Canadian General Standards Board, Sales Centre, Gatineau, Canada K1A 1G6. Telephone 819-956-0425 or 1-800-665-2472. Fax 819-956-5740. E-mail ncr.cgsb-ongc@tpsgc-pwgsc.gc.ca. Web site www.tpsgc-pwgsc.gc.ca/ongc-cgsb/index-eng.html.

[6] Canadian Standards Association (CSA). CAN/CSA-ISO/IEC 11179-3-13, *Information technology — Metadata registries (MDR) — Part 3: registry metamodel and basic attributes.* Available from: http://shop.csa.ca/

[7] Canadian Standards Association (CSA). CAN/CSA-ISO/IEC 14662-01, *Information technology — Open-EDI reference model.* Available from: http://shop.csa.ca/

[8] International Standards Organization (ISO). ISO/TR 13028 *Information and documentation – Implementation guideline for digitization of records.* Available from: IHS Markit. www.global.ihs.com/

[9] International Standards Organization (ISO). ISO 15489-1 *Information and documentation — Records management — Part 1: General.* Available from: IHS Markit. www.global.ihs.com/

[10] International Standards Organization (ISO). ISO/TR 15489-2 *Information and documentation — Records management — Part 2: Guidelines.* Available from: IHS Markit. www.global.ihs.com/

[11] International Standards Organization (ISO). ISO 15801 *Electronic imaging – Information stored electronically – Recommendations for trustworthiness and reliability.* Available from: IHS Markit. www.global.ihs.com/

[12] International Standards Organization (ISO). ISO 19005 *Document management –Electronic document file format for long-term preservation – Part 1: Use of PDF 1.4 (PDF/A-1).* Available from: IHS Markit. www.global.ihs.com/

[13] International Standards Organization (ISO). ISO 19005 *Document management – Electronic document file format for long-term preservation – Part 2: Use of ISO 32000-1 (PDF/A-2).* Available from: IHS Markit. www.global.ihs.com/

[14] International Standards Organization (ISO). ISO 19005 *Document management – Electronic document file format for long-term preservation – Part 3; Use of ISO 32000-1 with support for embedded files (PDF/A-3).* Available from: IHS Markit. www.global.ihs.com/

[15] International Standards Organization (ISO). ISO/IEC 27001 *Information technology – Security techniques – Information management systems – Requirements*. Available from: IHS Markit. www.global.ihs.com/

[16] International Standards Organization (ISO). ISO/IEC 27002 *Information technology – Security techniques – Code of practice for security controls.* Available from: IHS Markit. www.global.ihs.com/

[17] International Standards Organization (ISO). *ISO/IEC 27005 Information technology – Security techniques – Information security risk management.* Available from: IHS Markit. www.global.ihs.com/

[18] Sedona Canada. The Sedona Conference Working Group 7 (2015), *The Sedona Canada Principles Addressing Electronic Discovery* (Second Edition).