INTERNATIONAL STANDARD

ISO 18829

First edition
2017-06

Document management — Assessing ECM/EDRM implementations — Trustworthiness

Gestion de documents — Évaluation de la mise en oeuvre des ECM/EDRM — Fiabilité

Reference number
ISO 18829:2017(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword

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

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 171, *Document management applications*, Subcommittee SC 1, *Quality, preservation and integrity of information*.

Introduction

This document provides a methodology for organizations seeking to assess whether their ECM environment complies with key concepts of trustworthiness and information reliability as identified in ISO/TR 15801 and ISO/TR 22957.

Many organizations are now required to ensure their business-related electronically stored information (ESI) is securely created, stored and eventually destroyed in order to establish the authenticity and accuracy of the ESI and the security and trustworthiness of the organization.

This document identifies activities and operations an organization needs to follow in order to

— ensure that any electronically stored information (ESI) is created and maintained in a reliable and trustworthy manner through the entire ESI lifecycle, and

— evaluate existing enterprise content management (ECM) systems or electronic document and records management (EDRM) systems for compliance with applicable ISO standards.

ISO 15489, ISO/TR 15801 and ISO/TR 22957 provide organizations with guidance for the design of their enterprise content management (ECM) systems; however, organizations may also be required to provide auditable proof that these systems provide a secure environment for ESI that meets any legal, technical and policy obligations of the organization and comply with applicable ISO standards.

Any trustworthy ECM/EDRM solution needs to be capable of being audited, with reproducible results. There also needs to be a method of independently verifying the claims of the software and hardware vendors that the information is safe and secure and being stored in a trustworthy fashion. Organizations will need to ensure that their supporting documentation reflects these requirements.

Although standardized ECM solutions are likely to be auditable and can be easily verified, non-standardized or proprietary storage solutions may not provide a full audit trail and claims for the security of the ECM/EDRM solution made by vendors are difficult to independently verify. Regardless of whether the storage technology is standardized or proprietary, the organization faces the same need to be able to verify that the ECM/EDRM solution complies with all applicable requirements.

Document management — Assessing ECM/EDRM implementations — Trustworthiness

1 Scope

This document identifies activities and operations that an organization needs to perform, or have performed, to evaluate whether the electronically stored information (ESI) is or was maintained in a reliable and trustworthy environment(s). These environments utilize content or records management technologies commonly referred to as either enterprise content management (ECM) or electronic document and records management (EDRM) enforcing organizational records management policies and schedules.

ISO/TR 15801 and ISO 15489 (all parts) established the standards and best practices associated with implementing trustworthy records/document management environments. However, a standard is necessary to define the methodology used to evaluate these types of records/document management environments regardless of what technologies are currently employed by the organization. This document establishes the assessment methodology to be followed to identify the level of organizational compliance with these standards as related to trustworthiness and reliability of information stored in these environments.

This document is applicable to existing or planned ECM systems. Establishing the existence of a trustworthy system is an important step in documenting the reliability of ESI maintained within that system or environment. This document is designed for use by organizations evaluating the trustworthiness of existing record/document management environments. This document identifies all of the mandatory activities and areas that need to be examined by a resource, or resources, with a thorough technical and operational knowledge of the specific technologies and methodologies being examined, along with understanding record management processes and activities.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 12651-1, *Electronic document management — Vocabulary — Part 1: Electronic document imaging*

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

3 Terms and definitions

For the purposes of this document, the following terms and definitions given in ISO 12651-1, ISO 15489-1 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at http://www.iso.org/obp

3.1
authentic record
record that can be proven

a) to be what it purports to be,

b) to have been created or sent by the person purported to have created or sent it, and

c) to have been created or sent at the time purported

3.2
business practice documentation
BPD
detailed business process document identifying how information is received, stored and managed along with the processes, policies and procedures followed by the organization

Note 1 to entry: The BPD contains sufficient information allowing the organization to authenticate or certify that electronically stored information contained within the electronic document/record management system is accurate, reliable and trustworthy.

Note 2 to entry: In some areas, this document is referred to as a master procedure manual.

3.3
electronically stored information
ESI
information created, used and stored in digital form, and requiring a computer or other device for access

Note 1 to entry: For the purposes of this document, ESI includes documents and records created and/or managed by the organization in the course of business. Electronic data contained within relational databases or specialized application data sets are not considered to be part of the ESI examined when executing this assessment.

3.4
readability
ability of the system to accurately reproduce the stored information in a consistent fashion over a period of time without modification to the original content in any way that materially changes what was originally stored

3.5
reliable
trusted as a full and accurate representation of the transactions, activities or attested facts and can be depended upon in the course of subsequent transactions or activities

3.6
trustworthy
stored electronically in an accurate, reliable and usable/readable manner, ensuring integrity over time

Note 1 to entry: See ISO/TR 15801.

4 Trustworthy ECM system assessment

4.1 General

4.1.1 Assessment output

Trustworthy ECM systems shall ensure that information being managed can be reproduced in a reliable fashion and prevent unauthorized modifications or changes to the content or associated metadata. This includes any ESI generated from various office applications that utilize external sources to "complete" the document/record then created and/or printed/saved as determined appropriate by the organization.

The output of this standardized assessment shall include a detailed report including sufficient information allowing the organization to determine how to best address any areas identified as not being in full compliance. The report should also include, with detailed technology (if appropriate), recommendations and records/document management related policies and procedures required to come into full compliance.

A key element of this assessment standard is to provide detailed information to the organization related to the overall trustworthiness of their ECM environment along with recommendations on how to address those areas evaluated not to be in compliance with the associated ECM and records management related standards.

Upon conclusion of any ISO 18829-compliant assessment, the assessment team shall prepare a detailed report containing, at a minimum, the following:

— a business needs and/or business case. This section shall include a description of the records assessment process followed, a summary of findings for physical records and electronic records and business-related issues identified throughout the assessment;

— an analysis section that provides detailed information associated with a clear set of objective records and information management principles to achieve a measurable, consistent records information structure, fully insulated from individual and organizational bias. Previously referred to as GARP ("Generally Accepted Recordkeeping Principles"), it is now referred to within the records management industry as the "Principles" that define very specific levels of maturity of the records management program;

— a technology gap analysis section providing a description of all relevant ECM, records management and other document/record related storage or creation technologies currently in use by the organization;

— a section of technical and records related recommendations. This section shall include recommendations associated with changing the existing state of records management to establish a trustworthy ECM environment.

4.1.2 Process review

Any trustworthy ECM system assessment shall begin with a review of the processes and procedures associated with the entire environment in which ESI is managed. This includes reviewing not only the actual processes and procedures but also the business practices documentation (BPD). An evaluation shall be made regarding: how records, documents or information are ingested (i.e. how hardcopy is converted into electronic format, existing ESI is received and processed, etc.); how the system manages, audits and secures the electronic information; and how the system (including hardware) ensures that the storage of the information is secured, preventing unauthorized alteration, modification and/or deletion.

If the BPD is available, then the existing processes and procedures shall be verified against the documentation to determine compliance and/or areas in need of improvement including reviewing how

— all ECM procedures will be followed,

— information is or has been imported/scanned, indexed and verified,

— the system is and has been secured from unauthorized access,

— documents are and have been secured from unauthorized modification or alternation,

— authorized modification of document(s) has/have been and is/are managed, including audit trail information and the ability to retrieve any previous document version required to be maintained,

— notes and annotations (if any) have been and stored and managed, if they are a part of the business record, and

— the system establishes controls over all stored electronic information adhering to the published records retention schedule.

If a hosted solution or off-site components not within the direct custodial care of the organization are being utilized, the assessment team shall include reviewing the level of compliance with ISO 17068 Trusted Third Party Repositories. ISO 17068 provides detailed information and recommendations

associated with offsite vendor requirements, procedures and agreements that should be considered before storing content in an external environment that is not under the full control of the organization.

If the BPD is lacking or non-existent, the assessment can be followed by creating the documentation. The BPD is a required component of any trustworthy environment. While the creation of this document after the environment was placed into "production" may leave information contained in the system vulnerable to claims that it is not trustworthy, subsequently added information shall have a clearly documented process.

4.1.3 Fulfilling legal, government and regulatory requirements

Organizations that are subject to legal, government and regulatory requests for ESI may be required to verify the integrity and authenticity of the ESI under oath. Maintaining clearly defined policies and procedures and business practice documentation, as well as providing authenticated audit trails detailing how the ESI was collected and assembled, will be critical to establishing the authenticity of the ESI.

4.2 Assessment activities

4.2.1 Review of existing business practice and other organizational documentation

The assessment team shall examine the business practices document (BPD) previously developed to coherently explaining the interrelationship of the various organizational policies and procedures that impact the storage of electronic information.

Each of the areas covered by policies and procedures identified in the BPD shall be reviewed by the assessment team to determine whether the policies and procedures, together with the hardware, media and records/document management software has been implemented following design considerations identified in ISO/TR 22957, ISO/TR 15801 and ISO 15489. If the BPD does not exist, or is found to be lacking, the assessment team shall evaluate aspects of the ECM system, focusing on the policies and procedures related to how information is captured, managed and secured.

Furthermore, the assessment team shall review how the policies and procedures have been disseminated throughout the organization, including any training programs and ascertain the familiarity with them by the individuals charged with implementing or enforcing those policies.

Specifically, even if no BPD exists, the assessment team shall evaluate all the policies and procedures established under the principles identified in ISO/TR 15801 and ISO/TR 22957 regarding a trustworthy ECM system. Though the terms in these documents may differ slightly, the concept between key activities is consistent.

While the naming convention or existence of a particular policy or procedure is dependent upon the specific business operation, an assessment team could be expected to obtain and review policies and procedures in 4.2.2.

4.2.2 Evaluating information ingested into the system

4.2.2.1 General

The assessment team shall review in detail the processes associated with importing born digital data and information converted from hardcopy formats. The import, migration and/or conversion process(es) used to create ESI shall be reviewed in detail to ensure all information (as described in the BPD, if one exists, otherwise, the BPD needs to be developed; see 4.1.1) imported/converted and "indexed" is searchable and retrievable by all end-users upon request.

The assessment team shall prepare test scenarios from which the total number of pages and documents imported and/or converted can be compared and validated against the volume of information in original formats and structures.

4.2.2.2 Data conversion from hardcopy format into electronic format

The assessment team shall evaluate how documents were prepared for conversion and how the organization ensured that all documents, notes, etc. were converted from hardcopy format to ESI as described in the BPD. The assessment shall include examining whether users follow the processes and procedures, or which processes and procedures are not in conformance with international standards and best practices.

4.2.2.3 Born digital capture

This subclause deals with the capture of born digital data and storage in the ECM environment/solution being assessed. The assessment team shall evaluate the process used to capture data from external storage media to determine the following:

— the process utilized ensures all data anticipated to be stored in the trustworthy ECM solution was actually captured, indexed and stored as described in the policies and procedures;

— the process used to identify data duplication and/or replication between users who may have multiple copies of the same document;

— the process used for any existing content conversion from "out of date" or "proprietary" formats and how the user/migration team ensured all relevant data was converted without loss of fidelity or readability while ensuring all "material" information was converted as described in the BPD.

For data that required conversion, if some information was lost due to inability of conversion tool to convert as described in the BPD, the assessment team shall review whether the user/migration team also stored the original data in original format for historical purposes.

The assessment team shall identify and validate processes used during electronic information ingestion that required conversion from other formats in which the information was originally received.

4.2.3 Readability

Trustworthy ECM systems support the concept of ESI readability. Readability is the ability of the system to accurately reproduce the stored information in a consistent fashion over a period of time without unintended modification(s) to the original content in any way that materially changes what was originally stored.

The assessment team shall prepare test scenarios using a process of verifying readability of samples of the imported and/or converted information with standardized image/data "viewers". Proprietary or specialized "viewing" software shall not be used to verify readability of ESI, unless the proprietary or specialized "viewing" software is the only available software to access the ESI being evaluated. If this is the case, the evaluation team shall assess the "viewing" software from the perspective of availability into the future wherever possible. These test scenarios shall be executed by the system and the output examined by the assessment team for a "sampling of ESI" to

— determine whether there have been unintentional modifications to the ESI being managed by the system,

— enable the assessment team to evaluate whether the content between original document/record and the electronic version has changed,

— identify whether any specialized tools are required to extract/display the information that perform any interpolation or extrapolation of the data, and/or

— identify whether the ESI formats/structures are standardized and which standards are being followed.

4.3 Evaluating information retention, preservation and destruction

4.3.1 Application interoperability

Evaluate whether metadata used within the ECM system is duplicated between ECM systems, can be changed or modified changing accessibility to the ESI or preventing future accessibility and/or can produce different results depending on which system is used to search, store and/or retrieve ESI.

4.3.2 Data migration between electronic storage media

Evaluate how information was migrated into the ECM solution including procedures to ensure ESI and related metadata remained intact including file formats, compression, metadata, etc. Evaluate what type and level of auditing was implemented during the migration and how the organization determined that all anticipated ESI was migrated as described in the BPD.

4.3.3 Data format conversion

Evaluate the process utilized to convert the ESI from the original format to the desired format. Evaluate the methodology used to ensure no loss of information along with process documentation on the procedures followed to perform the conversion(s).

4.3.4 Media monitoring program

Evaluate the storage technology used for the ESI data and all documentation associated with how the stored information is secured and in compliance with relevant international standards associated with trustworthy storage environments (ISO/TR 15801, ISO/TR 22957, etc.).

4.3.5 Data expunging/deletion

Evaluate how the organization handles receipt of expunging requests and the formalized process to manage deletion of ESI flagged by the ECM system as either requiring archiving to an outside system or removal after the ESI has reached the end of its lifecycle.

The assessment team shall review the document retention policy and schedule to verify that appropriate ESI has been identified and the electronic retention scheduling portion of the ECM solution has been configured according to the schedule and policy. Along with reviewing this information, the team shall review all versions of the retention schedules and policies to determine if changes and updates are clearly identifiable and all information contained in the ECM solution is being managed as defined and documented. The assessment team should also review any manual records management processes that may exist in the absence (or instead) of an automated process.

Further, an assessment shall be made regarding how the retention schedule may be suspended so as to comply with discovery response procedures or litigation hold policies.

4.4 System security

4.4.1 Security-related information to be collected/reviewed

The organizational policies and procedures established to access, capture, manage and/or create ESI while maintaining trustworthiness and reliability shall be evaluated. The assessment team shall identify whether information captured, managed and secured by the system is captured (audit level history), documenting (both successful and unsuccessful) any attempted addition, modification or deletion of ESI during the information lifecycle along with other historical tracking of user activities.

This assessment shall include reviewing the technical architectures, the ECM software, storage media trustworthiness, including system and network security and whether sufficient system controls are in place to prevent unauthorized access to both the system and data maintained within the ECM storage environment.

The assessment team shall collect information from the organizational network team and/or infrastructure team to evaluate how the organizational network is secured from unauthorized access, both electronic and physical. Additionally, the assessment team shall evaluate the ECM solution to determine whether users are able to access ESI, database data, or other information associated with the ECM solution outside of established authorization and/or appropriate levels of security credentials.

4.4.2 Securing the information to prevent unauthorized modification or deletion of ESI

This step requires evaluation of both the system-level and document-level security features to determine what protections are in place to prevent unauthorized modifications or alterations to the ESI. At the system-level, the evaluation team shall sample existing audit history and logged historical information. This audit history and logged historical information should contain information related to login attempts (both successful and failed) along with data access attempts (both successful and failed).

At the document-level, the ESI shall be stored in ECM solutions that are configured to prevent unauthorized access, modification or deletion and provide audit trails verifying that the ESI has not been altered from its original form. Ensuring that unauthorized modification or alteration cannot take place once the ESI enters the system is the goal for most organizations. As not all ECM solutions provide this level of system and/or document level security and/or may not be configured as designed/planned, the overall solution shall be fully evaluated to determine compliance with organizational and records management policies and procedures.

4.5 Evaluating information access

4.5.1 General

Identify and document the steps taken to prevent unauthorized access to the ECM system. For example, housing of ESI on a network drive, even if protected by various security levels, may not be sufficient if the information can be accessed without an audit trail.

The assessment team needs to evaluate how ESI is stored in a secure environment where all access is fully logged and tracked, preventing any user from accessing the data through any non-logged modes/tools. This evaluation shall include a review of the process implemented by the organization to ensure that at least two (2) copies of the information have been committed to the storage media using techniques and optimizations that ensure exact copies of the information are created on multiple storage media in a timely way. The information should not be transferred to the storage media in ways that propagate data transfer errors, for example, by making copies in the absence of strict integrity controls.

The evaluation shall include reviewing the ECM system to confirm that errors in transferring data to all storage media are recorded and that there is a mechanism in place for fixing data transmission errors in a timely way. A record of successful ESI committals and failures to all storage media should be maintained, including any check-sums or other bit-comparative results, if created/used by the storage media (or sub-system).

The assessment team shall prepare test scenarios using a process of verifying that ESI is being stored to multiple locations, with at least one copy being stored in a storage technology that does not permit any modifications, alterations, or deletions outside the control of the records management system and/or trustworthy ECM controls. These test scenarios shall utilize a process of identifying a sampling of ESI to be examined to

— determine when the ESI is stored on the various storage media,

— evaluate ESI storage and system logging,

— examine the ability to access the ESI outside the controls provided by the ECM solution, and

— identify whether information can be altered or deleted through other means outside the controls provided by the ECM solution.

4.5.2 Managing authorized modification

4.5.2.1 General

Recognizing that there may be business reasons to allow modifications or alterations, it is critical to identify that these situations are the exception and not the rule and to identify policies and procedures to address when the changes may occur and whether they are followed. An audit trail should clearly identify the change, authorized user performing the change and the reason for the change.

4.5.2.2 Document classes, types and document access information

The processes and procedures related to how the ESI taxonomy and classification is documented and maintained shall be reviewed and verified as appropriate. The assessment team shall also verify whether changes and updates are clearly identifiable and all information contained in the ECM solution can be accessed and retrieved after the ECM solution was placed into production mode.

4.5.2.3 Document custodians

The assessment team shall review the training and experience levels of the document custodians to determine whether they understand the policies and how to apply them.

4.6 Evaluating history and audit trail information

4.6.1 General

Demonstrating consistency between the stated organizational policies and ECM or records related procedures that affect ESI is critical to establishing the accuracy of the information stored electronically and shall be part of establishing the audit trail.

For example, if information is described as being stored, managed and expunged in a specific manner, the failure to follow those policies casts doubt upon whether the information is being stored in a trustworthy system. Specifically, when a document retention policy and schedule (DRP/S) describes an expunging process such as all hard copy and electronic information shall be "removed" ("retired," "deleted," "destroyed" or some other similar phrase) yet employees state they are unaware or don't follow the process described in the DRP/S, the organization's claim to have a trustworthy repository is at risk because it can be demonstrated that it does not follow its own procedures regarding the handling of information. Further, the failure to follow the stated policies may expose the organization to substantial costs in producing and reviewing all information during litigation or regulatory investigations that it would otherwise have removed from its system.

4.6.2 to 4.6.4 identify various aspects of system logging and history that the assessment team should fully evaluate.

4.6.2 Retrieval of previous document version required to be maintained

If the ECM solution is configured to enable users to store documents utilizing version or revision controls, the organizational retention schedule/policy should clearly define when the system shall automatically remove versions or revisions of the document when the finalized document is approved.

For organizations that determine it is appropriate to maintain earlier versions of ESI, the system should provide a mechanism to locate and retrieve previous versions of the ESI and the system should log the fact that a new version of a document has been stored.

If the organization utilizes revision control (used after a document has been finalized) to keep track of updates to documents, the system should log when the newly revised document has been committed along with tracking other information such as date, time, reason for revision, user performing action, etc.

The assessment team shall evaluate how the organization manages document versions and/or revisions if being used within the ECM solution.

4.6.3 Management of notes and annotations as part of a business record

In some organizations and for some document/record types, notes and/or annotations should be retained with the same level of protections provided in the original document/record. Separating the note/annotation from the document/record to which it was associated, such as through the layering process, may not afford sufficient protections to deem that note/annotation to have been stored in a trustworthy system.

Careful evaluation of the methods for storing "layering" information is necessary within the context of the business needs. Associating the note/annotation with the original document/record in a traceable manner is required.

If the organization incorporates notes and/or annotations as part of a business process, automated processes through the use of workflow technologies, the assessment team shall evaluate the procedures followed by the organization.

The processes and procedures the assessment shall evaluate include those associated with how the organization:

— controls security associated with how notes and/or annotations are managed and stored;

— whether this information is under different retention controls;

— ensures sufficient audit log and historical information is managed by the ECM system identifying and logging all changes to any notes and/or annotations regardless if stored as part of the document or as part of a workflow process.

In the absence of any formal organizational documentation, the assessment team shall evaluate how the current ECM environment manages and secures this type of data through examining the existing ECM design and system level controls and provide recommendations to provide the necessary levels of controls.

The assessment team shall evaluate how the organization manages notes and/or annotations if being used within the ECM solution.

4.6.4 Management of ESI containing macros and/or external links

The traditional model of thinking, related to what types of documents/records stored within ECM system, was to only consider office documents, emails, faxes and scanned documents. The rapid integration of most applications with office applications to generate documents and/or emails requires that any trustworthy ECM system support the ability to save a copy of what has been generated by the application in an unalterable format such as PDF or other industry standardized format.

With these technology integrations, ESI now commonly is being generated by applications, along with other applications that may utilize "macros" (such as those that automatically insert the current date, or other field data within a document), or external links to other files on an internal network, or even a link to an external document outside the organization (i.e. an internet URL). This generated ESI is then commonly uploaded to the ECM solution for management.

The assessment team shall evaluate how the ECM solution manages

— electronic content created from applications,

— electronic content generated with the use of "macros" (code embedded in a document that executes when displayed or printed), and/or

— links to other documents external to the ECM solution.

4.7 Evaluating technical and data storage environments

4.7.1 Information security models

Prevention of unauthorized alterations/deletions during the lifecycle of the stored information is an essential feature of a trustworthy ECM system. The assessment team shall evaluate whether the information security model prevents alteration/deletions during the lifecycle of the stored information. The assessment team shall also examine the information security policies and configuration to determine at a minimum, whether

— all user access is fully secured,

— attempts to access the system from unauthorized users is logged,

— external connections to the system are encrypted and restricted to authorized users only using an encrypted VPN solution or other network technology preventing ESI from being accessed and/or transmitted in a fashion that could be intercepted,

— system configuration is established to implement role based access control which will allow authorized users necessary access to documents; this may include read, update, or other access levels, and/or

— only authorized users can add/remove/change user permissions within the trustworthy ECM environment.

4.7.2 Storage technologies assessment

The assessment team shall evaluate and examine the use of the current ESI storage. Assessment of the storage technologies/media in use shall include evaluating whether the ESI can be altered, for example, where a network drive is used, whether any variants of write-once-read-mostly (WORM) technologies are in place and whether storage technologies are being audited.

The assessment team shall evaluate whether ESI can be accessed outside of the controlling ECM solution and/or whether the ESI can be accessed and/or modified without appropriate logging, tracking and security controls along with determining if multiple copies are being written with at least one copy being stored in an unalterable state during the information lifecycle.

If a hosted solution or off-site components not within the direct custodial care of the organization are being utilized, the assessment team shall include reviewing the level of compliance with ISO 17068 trusted third party repositories associated with all relevant aspects of how the hosting vendor/solution functions, operates and is managed/secured from unauthorized access and/or modification of the ESI.

4.7.3 Technology standards being followed by organization

The assessment team will sample the ESI to identify data formats in use to determine whether the ESI formats follow industry standards along with compression standards to determine usability and readability into the future as the technologies continue to change.

4.7.4 Primary and secondary storage

A key concept to trustworthy storage concepts is the ability of any system to save at least two copies of the information in safe and separate locations (also considered the primary or secondary storage). The primary storage is considered to be the first storage location for the first copy of the ESI and the secondary location is where the organization is storing the second copy of the ESI. The assessment team

