ANSI/AIIM 25: 2012

Assessing Trusted Systems for Compliance with Industry Standards and Best Practices

Approved as:

American National Standard Institute (ANSI) Standards

November 14, 2012

ANSI American National Standards Institute

aiim® The Global Community of Information Professionals

ANSI/AIIM 25-2012
Copyright 2012 by AIIM International
1100 Wayne Avenue, Suite 1100
Silver Spring, MD 20910-5603 USA
Telephone: 301.587.8202
Fax: 301.597.2711
E-mail: aiim@aiim.org
Website: http://www.aiim.org
ISBN # 0-89258-428-9

ANSI/AIIM 25-2012

Standard for Information and Image Management

Assessing Trusted Systems for Compliance with Industry Standards and Best Practices

Prepared by AIIM

Approved as American National Standards Institute Standard:

November 14, 2012

Abstract:

This industry standard identifies the activities and operations an organization shall perform in order to evaluate whether the electronically stored information is maintained in reliable and trustworthy Enterprise Content (or Records) Management ECM (also referenced as EDMS, ERM, ERMS) systems.

Table of Contents

Foreword

(This foreword is not part of the American National Standard for Information and Image Management ANSI/AIIM 25-2012 — Standard Recommended Practice — Assessing Trusted Systems for Compliance with Industry Standards and Best Practices.

This standard is based on the concepts/principles outlined in ISO 15801, 15489, 22957 and AIIM ARP 1 – 2009, Section 5.3.3, it has become important for the creation of an industry standard associated with how to assess and evaluate all aspects of electronically stored document and records to determine the trustworthiness of the system and to establish the accuracy and reliability of the information returned from the system. This standard identifies the steps and activities necessary to determine whether the ECM system/solution is considered to follow the concepts defined in the above mentioned ISO standards related to Trusted ECM solution implementation and utilization.

Suggestions for improving this standard are welcome. They should be sent to the Chair, AIIM Standards Board, AIIM, 1100 Wayne Avenue, Suite 1100, Silver Spring, Maryland, 20910-5603.

At the time this recommended practice was approved, the Standards Board of AIIM had the following members:

Name of Representative	Organization
Rick Laxman	Church of Jesus Christ of Latter-Day Saints
Denise Bedford	Kent State University
Robert Blatt	EID, Inc.
Robert Breslawski	Eastman Park Micrographics
Chérie Ekholm	Microsoft
Betsy Fanning	AIIM
Duff Johnson	Net Centric USA
Stephen Levenson	U.S. District Courts Administrative Office
Thomas Pole	Vangent

This standard was approved the AIIM C27.3 Trustworthy Assessment Committee. At the time this standard was approved, the AIIM C27.3 Trustworthy Assessment Committee had the following members:

Name of Representative	**Organization**
Robert Blatt, Chair	EID
Richard Allen	Muse Mobile Systems
John Breeden	Old Dominion Energy Co-operative
Robert Breslawski	Eastman Park Micrographics
Skip Borland	SBIC
Jim Boyle	CA SOS
Jenny Chakonova	CA DGS

Tony DeGruy	City of Stockton
Corrol'll Driskell	KnowledgeLake
Virginia Jo Dunlap	EID
Robert Elefante	
Andrea Goethals	Harvard
Bob Hayes	Hyland Software
Rick Laxman	Church of Jesus Christ of Latter-day Saints
Stephen Levenson	US. District Courts Administrative Office
Alan Linden	EID
Rebekah Marshall	County of Riverside
Michael Matthews	Oregon Secretary of State
Norman Mooradian	Cook Arthur
Joyce Sayed	County of Sonoma
Vigi Gurushanta	eVIDA Group

INTRODUCTION

At every turn organizations need to create, capture and store business-related documents, records and information in a safe and secure fashion. From investors to authorities to daily transactional partners and to courts, everyone who comes in contact with an organization is relying upon the ability of that organization to establish the trustworthiness and accuracy of the electronically stored information (ESI). For example, some organizations regulated by the Securities and Exchange Commission, must follow rules 17 CFR 240.17a-3 and CFR 240.17a-4 that define non-alterable usage. California governmental entities must manage official records in compliance with relevant government codes and regulations that refer to the AIIM standards. Courts are now beginning to question the authenticity of the ESI evidence presented to them. At a minimum, organizations are recognizing the responsibility to ensure their business records are being created, captured and stored in a secure and trusted manner so that they are demonstrably reliable.

Under ISO 15489, ISO 15801 and AIIM ARP1-2009 organizations have a myriad of options for designing their Electronic Content Management (ECM) systems. However, an ECM system is not only comprised of the actual storage media, but also the firmware, application software, and policies and procedures that when integrated or combined provide an environment that enables organizations to create, capture, store, manage, and retrieve ESI with verifiable confidence that it has not been subject to inappropriate modifications, additions or deletions.

In order for any organization to manage and maintain electronic documents, records or information in a safe and secure trustworthy environment they must decide whether to use hardware/firmware media controls and/or software/policy controls to provide the desired storage environment. For example, the SEC has issued policy interpretations stating that the use alone of only software/policy based controls to provide non-alterability does not meet the tests for providing a trustworthy environment[1]. Other U.S. government agencies and regulatory bodies may have or will establish similar requirements for official document/record storage.

Therefore, organizations must provide safe and secure storage and information access, as well as have a mechanism to determine whether the solution actually meets the legal, technical and ethical obligations of the organization. This means that any storage solution must be "auditable" with reproducible results. There needs to be some 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. Standardized storage solutions are fully documented and can be easily verified. Non-standardized or proprietary storage solutions may, or may not be documented and the vendor information rarely can be independently verified. Regardless of whether the storage technology is standardized or proprietary, the organization faces the same dilemma: how to determine whether the system is functioning as designed and expected. Additionally, organizations must be more cognizant of the documentation prepared AND followed by the organization to both determine whether the Electronic Content Management (ECM) solution is actually safe and secure, creating a trustworthy document, record or information storage system and is providing the ability for the organization to monitor compliance with company record/document management policies.

[1] “SEC Interpretation: Electronic Storage of Broker Dealer Records”, Release No. 34-47806, US Securities and Exchange Commission. Effective May 12, 2003. This is available at www.sec.gov/rules/interp/34-47806.htm.

Assessing Trusted Systems for Compliance with Industry Standards and Best Practices

1 Scope and Purpose

1.1 Scope

The scope of this industry standard is to identify activities and operations an organization shall perform in order to evaluate whether the electronically stored information is maintained in reliable and trustworthy Enterprise Content (or Records) Management ECM (also referenced as EDMS, ERM, ERMS) systems. Using ISO 15801 section 5.1.1 , ISO 22957, and ARP 1 -2009 section 5.3.3 as a basis, this standard focuses on identifying factors that shall be considered when evaluating compliance with the relevant standards for an existing ECM system (or which shall be addressed during design of a new ECM system.) Establishing the existence of a trustworthy system is an important step in documenting the accuracy and reliability of the electronically stored information (ESI) maintained within that system or environment.

1.2 Purpose

The purpose of this industry standard is to identify activities and operations an organization shall follow in order to ensure that ESI is created, captured and maintained in a reliable and trustworthy manner by evaluating its existing ECM system. The concepts defined in this industry standard shall also be incorporated into the design of a new system.

1.3 Exclusion

This document is not intended to be an all-inclusive standard on assessing or evaluating whether an ECM solution is considered to be a "Trusted System" but rather to provide a methodology for organizations seeking to evaluate whether their ECM system complies with ISO 15801 and ARP 1 – 2009, Section 5.3.3 This document does not promote any technology or vendor’s product and it does not seek to provide legal guidance or legal opinions. Other types of trusted systems for digital content are not addressed in this standard.

2 Normative references

The following normative documents contain provisions which through reference in this text, constitute provisions of this standard. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies.

ISO/TR 15801, *Document management -- Information stored electronically -- Recommendations for trustworthiness and reliability*

AIIM ARP 1 – 2009 *Analysis, Selection, & Implementation of Electronic Document Management Systems (EDMS)*

3 Terms and definitions

For the purposes of this standard, the terms and definitions given in ISO 12651-1, ISO 15489 and ANSI/AIIM TR 2 and the following apply.

3.1 Trusted System

a system used to store electronic information in an accurate, reliable and usable / readable manner, ensuring integrity over time (See ISO 15801).

3.2 Authentic

the qualities of a document, record or other ESI that establishes the origin, reliability and trustworthiness of its content.

3.3 Electronic

relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.

3.4 Electronically Stored Information
ESI

ESI is digital information, regardless of the media or whether it is in the original format in which it was created.

4 Trusted System Assessment

4.1 General

Any Trusted System Assessment must begin with a review of the processes and procedures associated with the entire environment in which ESI is stored. 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 (e.g. how hardcopy is converted into electronic format); how the system manages, logs, tracks, and secures the electronic information; and how the system (including hardware) ensure the storage of the information is secured, preventing unauthorized alteration, modification and/or deletion.

If a 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. If the BPD is lacking or non-existent, the assessment can be followed by creating the documentation. While this may leave information contained in the system vulnerable to claims that it is not trustworthy, subsequently added information shall have a clearly documented process.

4.2 Assessment Activities

4.2.1 General

As a first step, the organizational business practice documentation shall be reviewed. This documentation should include information identified in ARP 1 – 2009 section 6.17 "Business Practice Documentation".

The assessment team shall review the BPD policies and procedures against the practices being followed by the user teams, as well as industry standards and best practices. Failure to follow the processes and procedures as described in the BPD, or which are not in conformance with industry standards and best practices, may leave an organization vulnerable to claims that the ESI is not reliable or accurate.

4.2.2 Review of Existing Business Practice Documentation or Procedures Manual

The assessment team shall examine the Business Practices Document or Procedures Manual (BPD/PM) previously developed to provide the framework for capturing and coherently explaining the interrelationship of the various organizational policies and procedures that impact the storage of electronic information.

Each of the policies and procedures identified in the BPD/PM shall be reviewed by the assessment team to determine whether the policies and procedures, together with hardware, media and software, have been followed since the ECM system was first placed into production. If the BPD/PM does not exist[2], 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.

Further, 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/PM exists, the assessment team shall evaluate all the policies and procedures established under the principles identified in ISO 15801 and ARP-1 2009 regarding a trusted ECM system. Table 1 – ISO 15801 and ARP 1 -2009 Cross Reference documents the relationship between the ISO 15801 system requirements with the associated detailed activities from ARP 1 -2009. It is important to note that when reviewing both documents that terms may be slightly different, but 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 the following categories:

Table 1 – ISO 15801 and AIIM ARP 1-2009 Cross Reference (ISO order)

ISO 15801	ARP-1 2009
— information capture (see ISO 15801, 6.3);	— description of how information will be scanned, indexed, and verified;
— document image capture (see ISO 15801, 6.4);	— description of how information will be scanned, indexed, and verified;
— data capture (see ISO 15801, 6.5);	— description of how information will be scanned, indexed, and verified;
— indexing (see ISO 15801, 6.6);	— description of how information will be scanned, indexed, and verified;
— authenticated output procedures (see ISO 15801,6.7);	— No Corresponding Section

[2] While the creation of the BPD/PM after the content/document management system has been placed into "production mode" may not enable the organization to demonstrate trustworthiness for ESI stored prior to documenting the processes, the assessment team's evaluation of the system, must enable the organization to prepare the BPD/PM and defend the ESI captured, managed, and secured after BPD creation.

— file transmission (see ISO 15801,);	— No Corresponding Section
— information retention (see ISO 15801, 6.9);	— description of how the system will adhere to the published records retention schedule; description of how the system will be secured from unauthorized access; unauthorized modification or alternation;
— information preservation (see ISO 15801, 6.10)	— description of how documents will be secured from unauthorized modification or alternation; description of how the system will adhere to the published records retention schedule; description of how authorized modification of documents will be managed, including audit trail; description of how notes and annotations (if any) will be stored and managed, if they are a part of the business record.
— information destruction (see ISO 15801, 6.11);	— description of how the system will adhere to the published records retention schedule
— backup and system recovery (see ISO 15801, 6.12);	— No Corresponding Section
— system maintenance (see ISO 15801, 6.13);	— description of how the system will be secured from unauthorized access;
— security and protection (see ISO 15801, 6.14)	— description of how the system will be secured from unauthorized access;
— use of contracted services (see ISO 15801, 6.15);	— No Corresponding Section
— workflow (see ISO 15801, 6.16)	— No Corresponding Section
— date and time stamps (see ISO 15801, 6.17);	— No Corresponding Section
— version control (see ISO 15801, 6.18);	— Information and the ability to retrieve any previous document version required to be maintained; description of how notes and annotations (if any) will be stored and managed, if they are a part of the business record.
— maintenance of documentation (see ISO 15801, 6.19).	— description of how these policies and procedures will be followed

4.2.3 Capture and Indexing

4.2.3.1 Data Conversion from hardcopy format into electronic format

The Assessment Team shall evaluate how documents were prepared for conversion and how the organization ensured all documents, notes, etc. were properly converted from hardcopy format to ESI as compared to description contained in the BPD/PM.

4.2.3.2 Data Migration Processes

This section deals with migration of data from existing storage media into the Trusted ECM solution. The Assessment team shall evaluate the process used to migrate data from external storage media to determine:

- the process utilized ensures all data anticipated to be migrated by the user was actually migrated and properly indexed and stored
- the process used to identify data duplication and/or replication between users who may have multiple copies of the same document
- the process used to convert data stored in "out of date" or "proprietary" formats into standardized structures and how the user/migration team ensured all relevant data was properly migrated without loss of fidelity, readability while ensuring all "material" information was properly migrated.

NOTE For data that required conversion, if some information was lost due to inability of conversion tool to properly convert, did the user/migration team also store the original data in original format for historical purposes)

4.2.4 Information Retention, Preservation, and Destruction

4.2.4.1 Application Interoperability.

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

4.2.4.2 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 industry standards associated with Trusted Storage systems (ISO 15801, ARP 1 – 2009 Section 5.3.3, etc.)

4.2.4.3 Data Expungement/Deletion.

Evaluate the formal procedure documentation related to how the organization handles receipt of expungement requests and the formalized process implemented by the records manager to manage removal of ESI. This evaluation shall include reviewing of systems logging and tracking specifically related to ESI deletion and/or expungement.

4.2.4.4 System Security

Policies and procedures implemented through content/document management software, storage media trustworthiness, system and network security shall be evaluated to identify whether information captured, managed and secured by the system are designed to prevent any unauthorized addition, modification, or deletion of ESI and the thoroughness of the audit trail. 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.

4.3 Evaluating Information ingested into the system

4.3.1 General

The assessment team shall review in detail the processes associated with importing born digital data and information converted from hardcopy formats. The import and/or conversion processes used to create ESI shall be reviewed in detail to ensure all information is properly imported/converted and "indexed" to ensure end-users are able to search and retrieve all anticipated information 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.

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.

4.3.2 Readability

Trusted 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 modification 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 utilize a process of identifying a "sampling of ESI" to be examined to:

- determine whether the ESI has been materially changed during loading/importing;
- 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
- identify whether the ESI formats/structures are standardized and which standards are being followed.

4.4 Evaluating Information Access

4.4.1 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 anyone could access the information 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 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 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 Trusted 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 logging and Trusted system logging;
- examine the ability to access the ESI "outside" the controls provided by the Trusted ECM solution;
- identify whether information can be altered or deleted through other means "outside" the controls provided by the ECM solution.

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 trusted ECM solutions that are configured to prevent unauthorized access, modification and/or deletion and which provide audit trails verifying that the ESI has not been altered from its original form. In the majority of organizations, ensuring that unauthorized modification or alteration cannot take place once the ESI enters the system is the goal. As not all ECM solutions provide this level of system and/or document level security and/or may not be properly configured, the overall solution shall be fully evaluated to determine compliance with organizational and records management policies and procedures.

4.4.3 Managing authorized modification

The evaluation team shall review relevant system and document logging history for a sampling of documents that have been modified by authorized users. This review shall include reviewing design documentation related to how the ECM system being evaluated prevents unauthorized access and/or modification, annotation or markup along with logging and tracking all changes to ESI after being committed into the ECM system.

4.4.3.1 Document Classes, Types and Document Access Information

The documentation associated with how the ESI taxonomy and classification is maintained shall be reviewed and verified as current. The assessment team shall also review all versions of the taxonomy document and verify that 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.

The assessment team shall also 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.

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.

4.4.3.2 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.

4.5 Evaluating History and Audit trail information

4.5.1 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.

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

In some organizations, notes or annotations to the ESI document/record are an integral part of how they do their business. Thus, the notes or annotations should be retained with the same level of protections provided 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 trusted 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.

4.5.3 Documenting consistency with stated policies

Demonstrating consistency between the stated policies 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 trusted system. Specifically, when a Document Retention Policy and Schedule (DRP/S) describes an expungement 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 trusted 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. In the US, substantial sanctions may also be imposed during litigation for these failures.[3]

Therefore, as part of determining whether an audit trail may be established, the assessment team must review the actual practices against the recorded processes.

4.6 Evaluating Technical and Data Storage Environments

4.6.1 Information Security Models

The assessment team shall 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 only allow authorized users access to various classes and types of documents including read, update, and other controls
- Only authorized users can add/remove/change user permissions within the Trusted ECM solution

4.6.2 Storage Technologies Assessment

The assessment team shall evaluate and examine the use of the current ESI storage technology being utilized. The storage technologies assessment shall include evaluating whether non-alterable or alterable storage is being used, how the ESI is stored in 2 safe and separate locations, and how the storage sub-system prevents unauthorized access or modification of any type.

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

4.6.3 Technology Standards being followed by organization

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

[3] Another area of risk to some organizations may be with ECM systems that only remove the pointers, which may be inaccurately described in the policies. Some organization could be exposed to legal sanctions and expensive recovery procedures because the stated policy and the ECM system don't match. Conflicts might also arise between the back-up protocols, the ECM system and the DRP/S, leading to confusion as to which policy is to be followed.

4.6.4 Primary and Secondary Storage

The assessment team will examine both the primary and secondary storage technologies to determine whether all ESI has been stored according to policies and procedures defined in the business practice documentation and in compliance with relevant industry standards and government codes/regulations

The assessment team will examine the various data storage locations to determine the processes utilized by the organization ensuring that:

- Two copies of the information is stored in separate physical locations
- At least one copy of the information is stored on a media that does not permit additions, deletions or changes to the original information.

5 Admissibility in Court

For organizations which are subject to litigation and regulatory oversight requests for ESI, particular attention should be paid to adherence to developing and maintaining a trusted ECM system. Those organizations will be regularly called upon to establish the authenticity of the ESI produced and may be required to "authenticate" the ESI under oath. Having individuals identified prior to the requests for ESI who are familiar with the ECM system including the policies and procedures and Business Practices Documentation, as well as how the ESI was collected and assembled, will be critical to establishing the authenticity of the ESI.

Annex A
(informative)
Trusted System and Legal Considerations

(Source: ARP-1:2009, 5.3.3 Trusted System and Legal Considerations)

Recognizing that all document management systems manage both electronic documents and records and acknowledging that not all documents become records, organizations may/must (depending on various regulations where appropriate and established) require the same level of system trustworthiness and reliability. Regardless of whether this data is called a "document", "record", or some other term used by the organization, all electronically stored information must be stored in a trusted environment when required and in compliance with the associated record retention schedule/plan.

Taking this into consideration and ensuring that all electronic information is stored and managed in a trustworthy and reliable fashion, compliance with the concepts contained within ISO 15801 and those related to records management policies contained in ISO 15489 Part 1 must be considered. This will ensure that both technical planning, design, and implementation along with records management policies and procedures result in the implementation and operation/management of a trustworthy and reliable document management system for all electronically stored information. It is important to note that a trustworthy system incorporates not only technology but also adherence to documented policies and procedures through all aspects of the design, development, and implementation project phases and be maintainable in an ongoing fashion after rollout into production.

A trusted document management system ensures that that all electronically stored information can be considered to be a true and accurate copy of the original information received regardless of original format. The trusted document management system must ensure that at least two (2) separate copies of the electronically stored information is created on electronic media and at a minimum must meet all the following conditions:

(a) The trusted document management system must utilize both hardware and media storage methodologies to prevent additions, modifications, or deletion of information to the original document or record during the approved lifecycle of the stored information; and

(b) Hardware and media storage methodologies used to store information in a trusted system shall be verifiable through independent audit processes; and

(c) The trusted document management system shall write at least one copy of the electronic document or record into electronic media that does not permit additions, deletions, or changes to the original document and that is to be stored and maintained in a safe and separate location.

It is important to note that trusted document management systems incorporate not only technology, but also require adherence to organizational policies ensuring proper electronic document or record handling, processing as required by the organization (typically documented in the record retention policy and schedule) and electronic document management software or application components. (Additional information related to all aspects of the trusted system are documented in ISO 15801.)