

# Integrating Records Management Requirements into Financial Management Information Systems (FMIS)

*Systems Requirements: Gap Analysis Tool*



International Records Management Trust

March 2006

## CONTENTS

	Page
Section One    Introduction	1
Section Two    Instructions and Examples	2
Section Three    The Gap Analysis Tool	9

**SECTION ONE**  
**INTRODUCTION**

The Tool provides a template for assessing the degree to which an existing Financial Management Information System (FMIS) meets the core set of system requirements for records management as presented in Module Five of the *Guide for Integrating Records Management Requirements into Financial Management Information Systems* (the *Guide*). The Tool, which makes it possible to identify major gaps in records management functionality, follows a business process driven analysis of the FMIS. It allows the analyst to record analysis comments about each of the core system requirements, while providing specific information on the rationale and scope for each requirement and advice on how the requirement can be implemented.

*The tool is designed for use by technical personnel, such as system developers, system auditors and electronic records managers, who are familiar with system analysis methodology and techniques. It is intended to supplement their other requirements analysis activities. Modules Two and Five in the Guide should be reviewed before using the tool in order to understand the origins and context of the tool and to get the most benefit from its use.*

The Tool can be printed and completed in hard-copy format. However, it is primarily intended to be used as an electronic document template using *Microsoft Word* or a compatible word processing application (eg *OpenOffice Writer*) to complete the information. Instructions on how to use the Tool, with examples, are provided in Section Two below. The Tool itself is divided into three main sections:

- ? The *Gap Analysis Overview* is used to provide a description of the organisation, the FMIS and the business processes that are being evaluated for compliance with the core system requirements for records management.
- ? The *Gap Analysis Summary* provides a concise view of how the FMIS scores (*compliant* or *not-compliant*) for each of the twenty-one core requirements.
- ? The *Detailed Gap Analysis* records the information that the analyst used in scoring a given requirement as *compliant* or *not compliant*. The template provides quotations from the ISO 15489 Records Management Standard and the DoD 5015.2 Standard for Electronic Records Management in order to define the scope and rationale for each core requirement and to give the analyst additional information and options on how the requirement should be integrated into the FMIS.

**SECTION TWO**  
**INSTRUCTIONS AND EXAMPLES**

## 2.1 Procedures for the Gap Analysis

The Gap Analysis involves the following steps:

- A Fill out the Gap Analysis Overview
- B Fill out the Analysis Comments for each core requirement in the Detailed Gap Analysis
- C Update the *Compliant / Not Compliant* scoring in the Gap Analysis Summary
- D Repeat steps B and C until the FMIS has been analysed for compliance with all twenty-one records management requirements.

### A Fill out the Gap Analysis Overview

The Gap Analysis Overview is used to describe the organisation, business process and technical architecture of the FMIS that is being evaluated. Using a business-process driven analysis methodology, it follows the flow of the information created and used by the FMIS to support a business processes (eg accounts payable). It identifies documents that need to be captured and managed as records (eg requisition forms) for each of the primary steps in the business process. This information is recorded in the 'Business Process and Records' row in the Gap Analysis Overview. The table below is an example of a Gap Analysis Overview:

<b>ORGANISATION</b>	Ministry of Public Works
<b>ORGANISATIONAL UNIT(S)</b>	Accounting Department
<b>BUSINESS PROCESS</b>	Accounts Payable
<b>FMIS DESCRIPTION</b>	The Accounting Department uses the Accounts Receivable and Payable module of the <i>Product XYZ Financials</i> system. The application data is stored in a <i>Product XYZ</i> database. The application is made available to a total of 15 departmental users by <i>Product XYZ</i> application server over a <i>Product XYZ</i> network. A <i>Product XYZ</i> production scanner is used to scan vouchers and receipts. These are then stored on a <i>Product XYZ</i> CD jukebox.

BUSINESS PROCESS AND RECORDS	PROCESS	RECORDS
	1. Raise Requisition	Requisition Form (FMIS data object)
	2. Obtain Goods and Services	Receipts (paper scanned to CD jukebox)
	3. Submit for Payment	Payment Voucher (paper in triplicate)
	4. Make Ledger Entry	Accounts Payable Ledger (FMIS data object)
ANALYSIS DATE(S)	March 7 – 9 , 2006	
ANALYSIS BY	John Doe	

## B Fill out the Analysis Comments for Each Core Requirement in the Detailed Analysis

Each business process and the records it creates needs to be assessed in order to ensure that the FMIS is compliant with the 21 core system requirements for records management. This should be done using standard system analysis techniques, for instance, reviewing vendor and system documentation, interviewing developers, administrators and users of the system, modelling system components and processes, and testing the functionality and features of the system. The result of the gap analysis assessment for each requirement should be recorded in the Analysis Comments row in each Detailed Requirements Analysis Table.

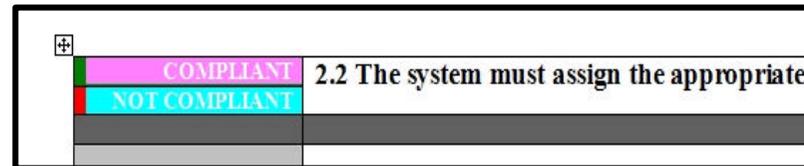
The table below provides an example of a Detailed Analysis. The analyst's comments are followed by quotations from the ISO 15489 Records Management Standard and the DoD 5015.2 Standard for Electronic Records Management relevant to the core requirement being addressed. These will help the analyst to assess whether or not the FMIS is compliant with the requirement being illustrated. The quotations under the heading **Implementation Consideration** provide specific examples of how the responses to the requirements can be implemented and deployed. The analyst also will need to draw on the concepts and guidelines presented in the *Guide to Integrating Records Management Requirements into Financial Management Information Systems*. In this example, the analyst decided that the FMIS was not compliant with the requirement.

<b>NOT COMPLIANT</b>	<b>2.2 The system must assign the appropriate retention and disposition rule to the record.</b>
<b>ANALYSIS COMMENTS</b>	<p>? The paper payment voucher is filed in a folder that is organised by calendar months. However, the accounts payable clerks are not marking any disposition codes or rules on the folders. One of the clerks noted that the folders are just cleared out from the filing cabinet and moved to the basement every couple of years or so when space becomes limited.</p> <p>? When the paper receipts are scanned to the CD jukebox they are assigned a unique identifier but no additional classification codes. As far as anyone can tell, they are kept permanently on these CDs (although they are only really required for a limited period of time).</p> <p>? A default seven-year retention rule is applied to the Accounts Payable Ledger. (At that time, the FMIS data is archived to a back-up tape). However, this is just based on common accounting practices and it has never been verified whether this is in fact the legal retention period for this organisation.</p>
<b>REQUIREMENT CITATIONS</b>	<p>'Any records created or captured need to have a retention period assigned, so it is clear how long they should be maintained.'  <i>ISO 15489-2, 4.2.4.2 Determining documents to be captured into a records system - p.11</i></p> <p>'The process requires reference to a disposition authority (see 4.2.4) of a more or less formal nature depending on the size and the nature of the organization and its accountabilities.'  <i>ISO 15489-2, 4.3.6 Identification of Disposition Status - p.17</i></p> <p>'All records within a records system should be covered by some form of disposition authority, from records of the smallest transactions to the documentation of the system's policies and procedures.'  <i>ISO 15489-2, 4.2.4.3 Determining how long to retain records - p.12</i></p> <p><b><u>Implementation Considerations</u></b></p> <p>'Many records systems, particularly electronic records systems, identify the disposition status and retention period of the record at the point of capture and registration. The process can be linked to activity-based classification and automated as part of system design.'  <i>ISO 15489-2, 4.3.6 Identification of Disposition Status - p.17</i></p>

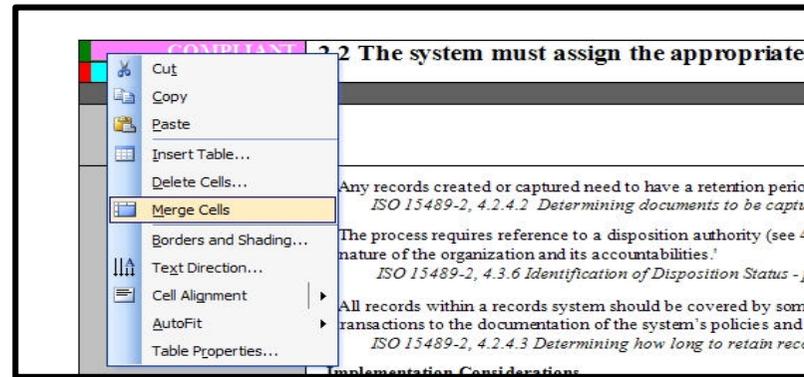
For each requirement covered by the Detailed Analysis Table, there is an option to select either compliant (green) or not compliant (red) in the left hand cell next to the core requirement. If the template is being completed in hard copy, the user can simply circle the correct score.

When using the electronic version, the analyst will delete either **COMPLIANT** or **NOT COMPLIANT** as appropriate in the following manner:

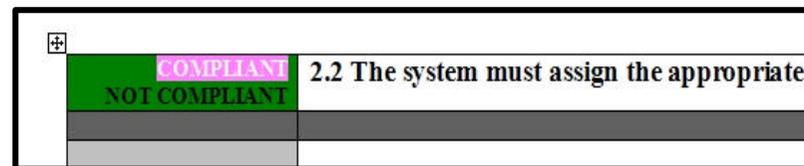
- 1 Select both the **COMPLIANT** and **NOT-  
COMPLIANT** cells (ie scroll over the two cells to highlight them).



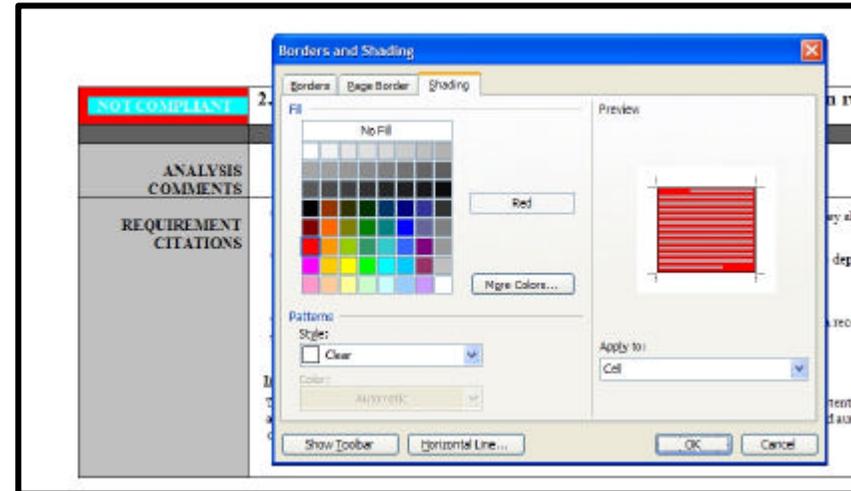
- 2 Use the Merge Cells option to blend them into a single cell (the cells will change colour when this is done).



- 3 Delete either **COMPLIANT** or **NOT COMPLIANT** as appropriate.



- 4 Right-click on the same table cell. Select the *Borders and Shading* option and choose the appropriate colour (red or green) from the colour palette. Ensure that the 'apply to' field indicates 'cell'.



When the Detailed Analysis is completed for a given core requirement, use the [\[back to top\]](#) link at the end of the Detailed Analysis Table to return to the Gap Analysis Summary (hold down the Ctrl key and click the link).

## **C Update the Compliant / Not Compliant Scoring in the Gap Analysis Summary**

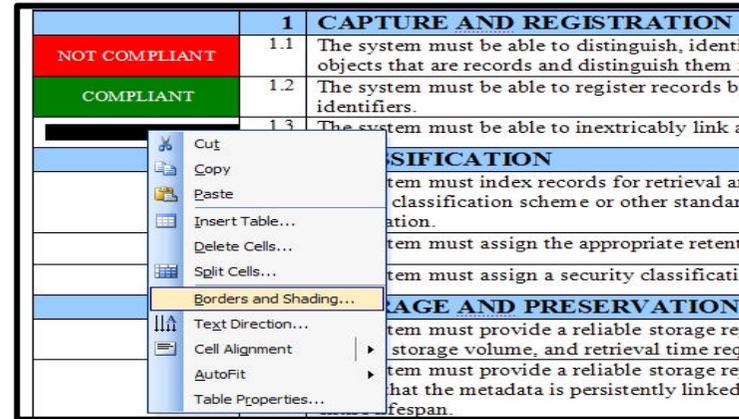
When the analyst has decided whether the FMIS is compliant or not-compliant with a given core requirement, this scoring should be added to the Gap Analysis Summary, which provides a high level view of the scores for each of the twenty-one core requirements and helps to identify major gaps in records management functionality. This table can be printed out and circulated to illustrate the final results of the gap analysis exercise. It can also provide a simple and highly effective quick reference tool that can be used in front of senior management audiences to show, at a glance, the level of risk the organisation is facing. Its effectiveness can be enhanced even further if it is produced in colour. The example below shows a Gap Analysis Summary for requirements 1.1 - 3.2:

COMPLIANCE	No.	CORE RECORDS MANAGEMENT REQUIREMENT	COMMENTS AND CITATIONS [Press Ctrl and Click Link]
	<b>1</b>	<b>CAPTURE AND REGISTRATION</b>	
NOT COMPLIANT	1.1	The system must be able to distinguish, identify and capture those documents or data objects that are records and distinguish them from non-record financial information.	<a href="#">Analysis Comments and Requirement Citations</a>
COMPLIANT	1.2	The system must be able to register records by assigning them unique identifiers that will remain with the records as long as the records exist.	<a href="#">Analysis Comments and Requirement Citations</a>
COMPLIANT	1.3	The system must be able to link contextual information (i.e. a metadata profile) to the record.	<a href="#">Analysis Comments and Requirement Citations</a>
	<b>2</b>	<b>CLASSIFICATION</b>	
COMPLIANT	2.1	The system must index records for retrieval and access using the organisation-wide records classification scheme or other standard taxonomies in use within the organisation.	<a href="#">Analysis Comments and Requirement Citations</a>
NOT COMPLIANT	2.2	The system must assign the appropriate retention and disposition rule to the record.	<a href="#">Analysis Comments and Requirement Citations</a>
COMPLIANT	2.3	The system must assign a security classification code to the record.	<a href="#">Analysis Comments and Requirement Citations</a>
	<b>3</b>	<b>STORAGE AND PRESERVATION</b>	
COMPLIANT	3.1	The system must provide a reliable storage repository that meets the records' requirements for file formats, storage volume, and retrieval time.	<a href="#">Analysis Comments and Requirement Citations</a>
NOT COMPLIANT	3.2	The system must provide a reliable storage repository for the records' metadata and ensure that the metadata is persistently linked to or embedded in the record for its entire lifespan.	<a href="#">Analysis Comments and Requirement Citations</a>

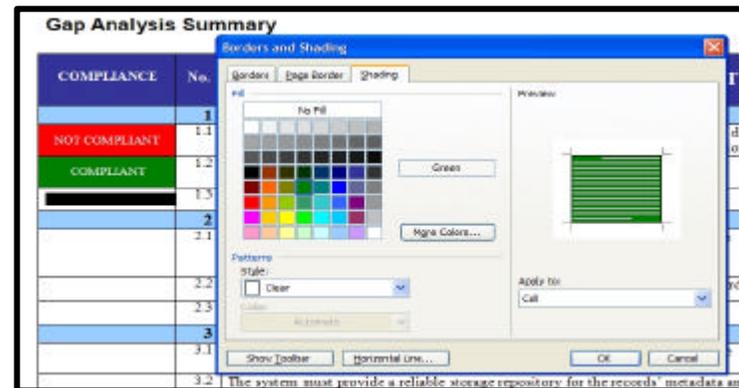
To navigate between the Detailed Analysis Table and the Summary Table, use the hyperlink in the right-hand column of the Summary Table. Hold down the Ctrl key and click the link.

To indicate **COMPLIANT** or **NOT COMPLIANT** in the Summary Table, use the formatting feature in the left-hand column as illustrated below:

- 1 Complete the detailed gap analysis for each of the requirements, right-click on the appropriate table cell under 'Compliance' and select the *Borders and Shading* option.



- 2 Select the appropriate colour (red or green) from the Shading palette and press OK. After the colour is selected, key in either **COMPLIANT** or **NOT COMPLIANT** in the cell. This is important because if the summary is printed out in black and white the reader will need to depend on the text in the cell to understand if it is system is compliant or non-compliant.



**SECTION THREE**  
**THE GAP ANALYSIS TOOL**

### 3.1 Gap Analysis Overview

<b>ORGANISATION</b>		
<b>ORGANISATIONAL UNIT(S)</b>		
<b>BUSINESS PROCESS</b>		
<b>FMIS DESCRIPTION</b>		
<b>BUSINESS PROCESS AND RECORDS</b>	<b>PROCESS</b>	<b>RECORDS</b>
<b>ANALYSIS DATE(S)</b>		
<b>ANALYSIS BY</b>		

## 3.2 Gap Analysis Summary

COMPLIANCE	No.	CORE RECORDS MANAGEMENT REQUIREMENT	COMMENTS AND CITATIONS [Press Ctrl and Click Link]
	<b>1</b>	<b>CAPTURE AND REGISTRATION</b>	
	1.1	The system must be able to distinguish, identify and capture those documents or data objects that are records and distinguish them from non-record financial information.	<a href="#">Analysis Comments and Requirement Citations</a>
	1.2	The system must be able to register records by assigning them unique identifiers that will remain with the records as long as the records exist.	<a href="#">Analysis Comments and Requirement Citations</a>
	1.3	The system must be able to link contextual information (i.e. a metadata profile ) to the record.	<a href="#">Analysis Comments and Requirement Citations</a>
	<b>2</b>	<b>CLASSIFICATION</b>	
	2.1	The system must index records for retrieval and access using the organisation-wide records classification scheme or other standard taxonomies in use within the organisation.	<a href="#">Analysis Comments and Requirement Citations</a>
	2.2	The system must assign the appropriate retention and disposition rule to the record.	<a href="#">Analysis Comments and Requirement Citations</a>
	2.3	The system must assign a security classification code to the record.	<a href="#">Analysis Comments and Requirement Citations</a>
	<b>3</b>	<b>STORAGE AND PRESERVATION</b>	
	3.1	The system must provide a reliable storage repository that meets the records' requirements for file formats, storage volume, and retrieval time.	<a href="#">Analysis Comments and Requirement Citations</a>
	3.2	The system must provide a reliable storage repository for the records' metadata and ensure that the metadata is persistently linked to or embedded in the record for its entire lifespan.	<a href="#">Analysis Comments and Requirement Citations</a>
	3.3	The system must provide backup and disaster recovery functionality for the record and records metadata storage repository.	<a href="#">Analysis Comments and Requirement Citations</a>
	3.4	The system must provide adequate security features to prevent unauthorised alteration or deletion of records or records metadata in the storage repository.	<a href="#">Analysis Comments and Requirement Citations</a>

	3.5	The system must be supported by a digital preservation plan that anticipates and establishes contingencies for technological obsolescence at the level of storage media, data formats, application software and hardware.	<a href="#">Analysis Comments and Requirement Citations</a>
	3.6	The system must document all data format and media migrations that are carried out on the records in their metadata profiles as part of their preservation history.	<a href="#">Analysis Comments and Requirement Citations</a>
	<b>4</b>	<b>ACCESS</b>	
	4.1	The system must provide the ability to search for, retrieve and display records.	<a href="#">Analysis Comments and Requirement Citations</a>
	4.2	The system must enforce user access and security restrictions.	<a href="#">Analysis Comments and Requirement Citations</a>
	<b>5</b>	<b>TRACKING</b>	
	5.1	The system must track the current location and custody of records, including checked-out records or copies of records.	<a href="#">Analysis Comments and Requirement Citations</a>
	5.2	The system must maintain secured audit logs on the access and use of records.	<a href="#">Analysis Comments and Requirement Citations</a>
	5.3	The system must establish version control and differentiate original records from drafts and copies.	<a href="#">Analysis Comments and Requirement Citations</a>
	<b>6</b>	<b>DISPOSITION</b>	
	6.1	The system must be able to calculate the retention period for records and trigger the appropriate disposition event when the retention period expires.	<a href="#">Analysis Comments and Requirement Citations</a>
	6.2	The system must be able to preserve those records that require long-term or permanent retention in accordance with a digital preservation plan (see Requirement 3.5) or transfer them to a storage repository that meets long-term preservation requirements.	<a href="#">Analysis Comments and Requirement Citations</a>
	6.3	The system must be able to completely and reliably expunge those records that have been assigned 'destruction' as their final disposition action (including any backup, reference or source copies).	<a href="#">Analysis Comments and Requirement Citations</a>
	6.4	The system must document retention information and disposition events in the record's metadata profile.	<a href="#">Analysis Comments and Requirement Citations</a>

### 3.3 Detailed Gap Analysis

1. CAPTURE AND REGISTRATION	
	<p>'Business or personal actions should be captured as records when they commit an organization or individual to action, render an organization or individual accountable, or document an action, a decision or decision-making process.' <i>ISO 15489-1, 9.1 Determining documents to be captured into a records system - p.11</i></p> <p>'Capture is the process of determining that a record should be made and kept. This includes both records created and received by the organization.' <i>ISO 15489-2, 4.3.2 Capture - p.14</i></p> <p><b><u>Implementation Considerations</u></b></p> <p>'In electronic records systems, the determinations about capture and retention should be considered in system design at the <i>ISO 15489-2, 4.2.4 Records disposition authority - p.10</i></p> <p>'Information systems, business applications and communication systems, and the business processes which they support, should be designed, modified or redesigned so that adequate records can be created and captured as a routine part of undertaking <i>ISO 15489-1, 8. Design and implementation of a records system - p.8</i></p>

<b>COMPLIANT</b>	<b>1.1 The system must be able to distinguish, identify and capture those documents or data objects that are records and distinguish them from non-record financial information.</b>
<b>NOT COMPLIANT</b>	
<b>ANALYSIS COMMENTS</b>	
<b>REQUIREMENT CITATIONS</b>	<p>'Strategies adopted by an organization for documenting its business activity should determine what records are required and when, how and where they should be captured into records systems.'  <i>ISO 15489-1, 8. Design and implementation of a records system - p.8</i></p> <p>'Records identified for continuing retention are likely to be those which:</p> <ul style="list-style-type: none"> <li>- provide evidence and information about the organization's policies and actions,</li> <li>- provide evidence and information about the organization's interaction with the client community it serves,</li> <li>- document the rights and obligations of individuals and organizations,</li> <li>- contribute to the building of an organization's memory for scientific, cultural or historical purposes, and</li> <li>- contain evidence and information about activities of interest to internal and external stakeholders.'</li> </ul> <p><i>ISO 15489-1, 9.2 Determining how long to retain records -p.12</i></p> <p><b><u>Implementation Considerations</u></b></p> <p>'Records of some transactions within a system are repeatedly used to perform further transactions. A distinction needs to be made between the core records, which are those used repeatedly, and records of multiple individual transactions, which refer to the core records; it may be possible to remove the individual transaction records from the system shortly after the transaction is completed. For example, leave records in personnel systems are only maintained for a limited period, while the leave history will be maintained as long as the employee is employed. The relationship between core business records and other transactional records will determine how long each are needed within the system. This is also dependent on the nature of the business activity being documented.</p> <p>For example, transaction records relating to a person's medical history may need to be retained longer than the accounts  <i>ISO 15489-2, 4.2.4.3 Determining how long to retain records - p.11-12</i></p>

[\[back to top\]](#)

<b>COMPLIANT</b>	<b>1.2 The system must be able to register records by assigning them unique identifiers that will remain with the records as long as the records exist.</b>
<b>NOT COMPLIANT</b>	
<b>ANALYSIS COMMENTS</b>	
<b>REQUIREMENT CITATIONS</b>	<p>'[Registering records is the] act of giving a record a unique identifier on its entry into a system.'  <i>ISO 15489-1, 3.18 Terms and definitions - p.3</i></p> <p>'RMA [Records Management Applications] shall assign a unique computer-generated record identifier for each record they manage regardless of where that record is stored'  <i>DoD 5015.2 (v.2, 2002), C2.2.3. Declaring and Filing Records - C2.2.3.5</i></p> <p>'An element of metadata, a record identifier is a data element whose value is system-generated and that uniquely identifies a particular record. (C2.T3.1 - Unique Record Identifier - mandatory, system generated, not editable)'  <i>DoD 5015.2 (v.2, 2002), DLI. DEFINITIONS - DLI.1.69.</i></p> <p>'The primary purpose of registration is to provide evidence that a record has been created or captured in a records system, and an additional benefit is that it facilitates retrieval.'  <i>ISO 15489-1, 9.4 Registration - p.13</i></p>

[\[back to top\]](#)

<b>COMPLIANT</b>	<p><b>1.3 The system must be able to link contextual information (i.e. a metadata profile) to the record, using at least the following attributes:</b></p> <ul style="list-style-type: none"> <li><b>a) unique record identifier</b></li> <li><b>b) date and time of record registration</b></li> <li><b>c) record creation date</b></li> <li><b>d) record title or description</b></li> <li><b>e) name of record creator or name of record user who captured the record</b></li> </ul>
<b>NOT COMPLIANT</b>	
<b>ANALYSIS COMMENTS</b>	
<b>REQUIREMENT CITATIONS</b>	<p>'Systems that capture records also need to capture metadata associated with the record.'  <i>ISO 15489-2, 4.3.2 Capture - p.14</i></p> <p>'Registration specifies the following metadata as a minimum:  a) unique identifier assigned from the system;  b) the date and time of registration;  c) a title or abbreviated description;  d) the author (person or corporate body), sender or recipient'  <i>ISO 15489-2, 4.3.3 Registration - p.15</i></p> <p>'Mandatory record metadata components are shown in Table C2.T3:  C2.T3.1. Unique Record Identifier  C2.T3.3 Subject or Title  C2 T3.4 Media Type  C2 T3.5 Format  C2 T3.6 Date Filed  C2.T3.7 Publication Date  C2.T3.9 Author or Originator  C2.T3.12 Origination Organization'  <i>DoD 5015.2 (v.2, 2002), C2.2.3. Declaring and Filing Records - C2.2.3.2.</i></p>

### **Implementation Considerations**

'Electronic records systems can be designed to register records through automatic processes, transparent to the user of the business system from which it is captured and without the intervention of a records management practitioner. Even where registration is not totally automated, elements of the registration process (specifically some of the metadata that are required for registration) can be automatically derived from the computing and business environment from which the record originates.'  
*ISO 15489-2, 4.3.3. Registration - p.15*

'RMA [Records Management Applications] shall (for all records) capture, populate, and/or provide the user with the capability to populate the metadata elements before filing the record. RMA [Records Management Applications] shall ensure that fields designated mandatory for data collections are non-null before filing the record.

*DoD 5015.2 (v.2, 2002), C2.2.3. Declaring and Filing Records - C2.2.3.10*

'For records that are being filed via the user interface, RMA [Records Management Applications] shall provide the user with the capability to edit the record metadata prior to filing the record, except for data specifically identified in this Standard as not editable. For autofiling, RMA [Records Management Applications] shall provide the user the option of editing the record metadata prior to filing.'

*DoD 5015.2 (v.2, 2002), C.2.2.3 Declaring and Filing Records - C2.2.3.11.*

'RMA [Records Management Applications] shall link the record metadata to the record so that it can be accessed for display, export, etc.'

*DoD 5015.2 (v.2, 2002), C2.2.3. Declaring and Filing Records - C2.2.3.21.*

'More detailed registration links the record to descriptive information about the context, content and structure of the record and to other related records. Depending on the nature of the business recorded, the organization's evidence requirements and technology deployed, the information attached to the record's unique identifier can include:

- a) document name or title,
- b) text description or abstract,
- c) date of creation,
- d) date and time of communication and receipt,
- e) incoming, outgoing or internal,
- f) author (with his/her affiliation),
- g) sender (with his/her affiliation),
- h) recipient (with his/her affiliation),
- i) physical form,
- j) classification according to the classification scheme,
- k) links to related records documenting the same sequence of business activity or relating to the same person or case, if the record is part of a case file,
- l) business system from which the record was captured,
- m) application software and version under which the record was created or in which it was captured.

	<ul style="list-style-type: none"><li>n) standard with which the records structure complies (for example, Standard Generalized Markup Language -- SGML, Extensible Markup Language- XML),</li><li>o) details of embedded document links, including applications software and version under which the linked record was created,</li><li>p) templates required to interpret document structure,</li><li>q) access,</li><li>r) retention period, and</li><li>s) other structural and contextual information useful for management purposes.</li></ul> <p><i>ISO 15489-2, 4.3.3 Registration - pp.15-16</i></p>
--	--

[\[back to top\]](#)

2. CLASSIFICATION	
	<p>'Classification is the process of identifying the category or categories of business activity and the records they generate and of grouping them, if applicable, into files to facilitate description, control, links and determination of disposition and access status.' <i>ISO 15489-2, 4.3.4 Classification - p.16</i></p> <p>'RMAs shall provide the capability to associate the attributes of one or more record folder(s) to a record, or for categories to be managed at the record level, provide the capability to associate a record category to a record.' <i>DoD 5015.2 (v.2, 2002), C2.2.3. Declaring and Filing Records - C2.2.3.1.</i></p> <p>'The degree of refinement of a classification system is at the discretion of the organization and reflects the complexity of the function undertaken within the organization.' <i>ISO 15489-2, 4.2.2 Business activity classification - p.9</i></p> <p><b><u>Implementation Considerations</u></b></p> <p>'The file/record is best classified at the same time as it is registered.' <i>ISO 15489-2, 4.3.3 Registration - p.16</i></p> <p>'Organizations need to determine the degree of classification control they require for their business purposes.' <i>ISO 15489-1, 9.5.2 Classification systems - p.13</i></p> <p>'RMAs shall provide the capability for only authorized individuals to create, edit, and delete file plan components and their identifiers.' <i>DoD 5015.2 (v.2, 2002), C2.2.1. Implementing File Plans - C2.2.1.1.</i></p>

<b>COMPLIANT</b>	<b>2.1 The system must index records for retrieval and access using the organisation-wide records classification scheme or other standard taxonomies in use within the organisation.</b>
<b>NOT COMPLIANT</b>	
ANALYSIS COMMENTS	

## REQUIREMENT CITATIONS

'The allocation of indexing terms may be restricted to the terminology established in the classification scheme or other vocabulary controls. Indexing terms are commonly derived from:

- a) the format or nature of the record,
- b) the title or main heading of the record,
- c) the subject content of the record, usually in accord with the business activity,
- d) the abstract of a record,
- e) dates associated with transactions recorded in the record,
- f) names of clients or organizations,
- g) particular handling or processing requirements,
- h) attached documentation not otherwise identified, or
- i) the uses of the records.'

*ISO 15489-2, 4.3.4.3 Indexing - p.17*

'Further descriptive and control details can be attached to the record by using vocabulary controls such as a list of authorized headings or a thesaurus (see 4.2.3.1 and 4.2.3.2).'

*ISO 15489-2, 4.3.4.2 Vocabulary controls - p.16*

'RMAs shall provide the capability to sort, view, save, and print user-selected portions of the file plan, including record folders.'

*DoD 5015.2 (v.2, 2002), C2.2.1. Implementing File Plans - C2.2.1.6.*

'Supported by instruments such as vocabulary controls, classification systems promote consistency of titling and description to facilitate retrieval and use'

*ISO 15489-2, 4.2.2 Business activity classification - p.8*

'Appropriate allocation of index terms extends the possibilities of retrieval of records across classifications, categories and media.'

*ISO 15489-2, 4.3.4.3 Indexing - p.16*

### **Implementation Considerations**

'Indexing can be done manually or be automatically generated. It may occur at various levels of aggregation within a records

*ISO 15489-1, 9.5.4 Indexing - p.14*

[\[back to top\]](#)

<p style="text-align: center;"><b>COMPLIANT</b></p> <p style="text-align: center;"><b>NOT COMPLIANT</b></p>	<p><b>2.2 The system must assign the appropriate retention and disposition rule to the record.</b></p>
<p style="text-align: center;"><b>ANALYSIS COMMENTS</b></p>	
<p style="text-align: center;"><b>REQUIREMENT CITATIONS</b></p>	<p>'Any records created or captured need to have a retention period assigned, so it is clear how long they should be maintained.'  <i>ISO 15489-2, 4.2.4.2 Determining documents to be captured into a records system - p.11</i></p> <p>'The process requires reference to a disposition authority (see 4.2.4) of a more or less formal nature depending on the size and nature of the organization and its accountabilities.'  <i>ISO 15489-2, 4.3.6 Identification of Disposition Status - p.17</i></p> <p>'All records within a records system should be covered by some form of disposition authority, from records of the smallest transactions to the documentation of the system's policies and procedures.'  <i>ISO 15489-2, 4.2.4.3 Determining how long to retain records - p.12</i></p> <p><b><u>Implementation Considerations</u></b></p> <p>'Many records systems, particularly electronic records systems, identify the disposition status and retention period of the record at the point of capture and registration. The process can be linked to activity-based classification and automated as part of system design.'  <i>ISO 15489-2, 4.3.6 Identification of Disposition Status - p.17</i></p>

[\[back to top\]](#)

<b>COMPLIANT</b>	<b>2.3 The system must assign a security classification code to the record.</b>
<b>NOT COMPLIANT</b>	
<b>ANALYSIS COMMENTS</b>	
<b>REQUIREMENT CITATIONS</b>	<p>'Organizations should have formal guidelines regulating who is permitted access to records and in what circumstances.'  <i>ISO 15489-1, 9.7 Access - p.14</i></p> <p>'The more complex the organization and the more complex its business and regulatory environment, the greater the need for standardization of procedures to apply access and security categories to records.'  <i>ISO 15489-2, 4.2.5 Security and access classification scheme - p.12</i></p>

[\[back to top\]](#)

### 3. STORAGE AND PRESERVATION

'The decision to capture a record implies an intention to store it.'

*ISO 15489-2, 4.3.7.1 Record Storage Decisions - p.18*

'Appropriate storage environment and media, physical protective materials, handling procedures and storage systems should be considered when designing the records system.'

*ISO 15489-1, 8.3.3 Physical storage medium and protection - p.9*

'RMAs should provide additional features for managing boxes of hard-copy records and other off-line archives.'

*DoD 5015.2 (v.2, 2002), C3.2. Other Useful RMA Features - C3.2.17.*

'Records of continuing value, irrespective of format, require higher quality storage and handling to preserve them for as long as that value exists.'

*ISO 15489-2, 4.3.9.2 Continuing Retention - p.20*

'Records identified for continuing retention need to be stored in environments conducive to their long-term preservation.'

*ISO 15489-2, 4.3.9.2 Continuing Retention - p.20*

'RMAs shall manage and preserve any record in any supported repository, regardless of its format or structure, so that, when retrieved, it can be reproduced, viewed, and manipulated in the same manner as the original.'

*DoD 5015.2 (v.2, 2002), C.2.2.5 Storing Records - C2.2.5.3.*

'Since RMAs are prohibited (see subparagraph C2.2.3.8.) from altering the format of stored records, the organization shall ensure that it has the ability to view, copy, print, and, if appropriate, process any record stored in RMAs for as long as that record must be retained.'

*DoD 5015.2 (v.2, 2002), C2.2.10. Additional Baseline Requirements. - C2.2.10.3.*

[\[back to top\]](#)

<p style="text-align: center;"><b>COMPLIANT</b></p> <p style="text-align: center;"><b>NOT COMPLIANT</b></p>	<p style="text-align: center;"><b>3.1 The system must provide a reliable storage repository that meets the records' requirements for file formats, storage volume, and retrieval time.</b></p>
<p style="text-align: center;"><b>ANALYSIS COMMENTS</b></p>	
<p style="text-align: center;"><b>REQUIREMENT CITATIONS</b></p>	<p>'Records should be stored on media that ensure their useability, reliability, authenticity and preservation for as long as they are needed. Records require storage conditions and handling processes that take into account their specific physical and chemical <i>ISO 15489-1, 9.6 Storage and handling - p.14</i></p> <p>'Records that are particularly critical for business continuity may require additional methods of protection and duplication to ensure accessibility in the event of a disaster.' <i>ISO 15489-2, 4.3.7.1 Record Storage Decisions - p.18</i></p> <p>'The system shall provide the capability to rebuild from any backup copy, using the backup copy and all subsequent system <i>DoD 5015.2 (v.2, 2002), C2.2.9. System Management Requirements - C2.2.9.4.</i></p> <p>'The system shall provide for the monitoring of available storage space. The storage statistics shall provide a detailed accounting of the amount of storage consumed by RMA processes, data, and records. The system shall notify individuals of the need for corrective action in the event of critically low storage space.' <i>DoD 5015.2 (v.2, 2002), C2.2.9. System Management Requirements - C2.2.9.5.</i></p> <p><b><u>Implementation Considerations</u></b></p> <p>'Knowing how long the records will need to be kept and maintained will affect decisions on storage media.' <i>ISO 15489-1, 8.3.3 Physical storage medium and protection - p.9</i></p> <p>'The purpose served by the record, its physical form and its use and value will dictate the nature of the storage facility and services required to manage the record for as long as it is needed.' <i>ISO 15489-2, 4.3.7.1 Record Storage Decisions - p.18</i></p> <p>'In some cases, where the legal and regulatory environment allows this, records may be physically stored with one organization, but the responsibility and management control reside with either the creating organization or another appropriate authority.'</p>

	<p>Such arrangements, distinguishing between storage, ownership and responsibility for records, are particularly relevant for records in electronic records systems. Variations in these arrangements may occur at any time in the systems' existence, and any changes to these arrangements should be traceable and documented.'</p> <p><i>ISO 15489-1, 8.3.4 Distributed management - p.10</i></p>
--	--

[\[back to top\]](#)

<b>COMPLIANT</b>	<b>3.2 The system must provide a reliable storage repository for the records' metadata and ensure that the metadata is persistently linked to or embedded in the record for its entire lifespan.</b>
<b>NOT COMPLIANT</b>	
<b>ANALYSIS COMMENTS</b>	
<b>REQUIREMENT CITATIONS</b>	<p>'Metadata [is] data describing context, content and structure of records and their management through time.'</p> <p><i>ISO 15489-1, 3. Terms and definitions , p.3</i></p> <p>'As well as the content, the record should contain, or be persistently linked to, or associated with, the metadata necessary to document a transaction'</p> <p><i>ISO 15489-1, 7.2.1 General, p.7</i></p> <p>'Business or personal actions should be captured as records <i>and linked with metadata which characterize their specific business context</i> when they commit an organization or individual to action, render an organization or individual accountable, or document an action, a decision or decision-making process.'</p> <p><i>ISO 15489-1, 9.1 Determining documents to be captured into a records system - p.11</i></p> <p>'RMAs shall, for records approved for accession and that are not stored in an RMA supported repository, copy the associated metadata for the records and their folders to a user-specified filename, path, or device.'</p> <p><i>DoD 5015.2 (v.2, 2002), C2.2.6.5. Transferring Records – C2.2.6.5.3.</i></p>

[\[back to top\]](#)

<b>COMPLIANT</b>	<b>3.3 The system must provide backup and disaster recovery functionality for the record and records metadata storage repository.</b>
<b>NOT COMPLIANT</b>	
<b>ANALYSIS COMMENTS</b>	
<b>REQUIREMENT CITATIONS</b>	<p>'The RMA system shall provide the capability to automatically create backup or redundant copies of the records and their metadata <i>DoD 5015.2 (v.2, 2002), C2.2.9. System Management Requirements - C2.2.9.1.</i></p> <p>'The system shall provide the capability to rebuild from any backup copy, using the backup copy and all subsequent system <i>DoD 5015.2 (v.2, 2002), C2.2.9. System Management Requirements - C2.2.9.4.</i></p> <p>'Storage conditions and handling processes should be designed to protect records from unauthorized access, loss or destruction, and from theft and disaster.' <i>ISO 15489-1, 9.6 Storage and handling - p.14</i></p> <p>'The records system should address disaster preparedness to ensure that risks are identified and mitigated.' <i>ISO 15489-1, 8.3.3 Physical storage medium and protection - p.9</i></p> <p>'Records that are particularly critical for business continuity may require additional methods of protection and duplication to ensure accessibility in the event of a disaster.' <i>ISO 15489-2, 4.3.7.1 Record Storage Decisions - p.18</i></p> <p><b><u>Implementation Considerations</u></b></p> <p>'The method used to back up RMA database files shall provide copies of the records and their metadata that can be stored off-line and at separate location(s) to safeguard against loss due to system failure, operator error, natural disaster, or willful <i>DoD 5015.2 (v.2, 2002), C.2.2.9. System Management Requirements - C2.2.9.2.</i></p> <p>'Integrity should be demonstrably maintained during and after recovery from disaster.' <i>ISO 15489-1, 8.3.3 Physical storage medium and protection - 9</i></p> <p>'Following any system failure, the backup and recovery procedures provided by the system shall: C2.2.9.3.1. Ensure data integrity by providing the capability to compile updates (records, metadata, and any other I</p>

	<p>information required to access the records) to RMAs.  C2.2.9.3.2. Ensure these updates are reflected in RMA files, and ensuring that any partial updates to RMA files are separately identified. Also, any user whose updates are incompletely recovered, shall, upon next use of the application, be notified that a recovery has been attempted. RMAs shall also provide the option to continue processing using all in-progress data not reflected in RMA files.'</p> <p style="text-align: center;"><i>DoD 5015.2 (v.2, 2002), C2.2.9. System Management Requirements - C2.2.9.3.</i></p>
--	--

[\[back to top\]](#)

<b>COMPLIANT</b>	<b>3.4 The system must provide adequate security features to prevent unauthorised alteration or deletion of records or records metadata in the storage repository.</b>
<b>NOT COMPLIANT</b>	
<b>ANALYSIS COMMENTS</b>	
<b>REQUIREMENT CITATIONS</b>	<p>'RMAs shall prevent subsequent changes to electronic records stored in its supported repositories. The content of the record, once filed, shall be preserved.'  <i>DoD 5015.2 (v.2, 2002), C2.2.3. Declaring and Filing Records - C2.2.3.8.</i></p> <p>'The RMAs shall prevent unauthorized access to the repository(ies).'  <i>DoD 5015.2 (v.2, 2002), C2.2.5. Storing Records. - C2.2.5.2.</i></p> <p>'The integrity of a record refers to its being complete and unaltered. It is necessary that a record be protected against unauthorized alteration.'  <i>ISO 15489-1, 7.2.4 Integrity - p.7</i></p> <p>'To ensure the authenticity of records, organizations should implement and document policies and procedures which control the creation, receipt, transmission, maintenance and disposition of records to ensure that records creators are authorized and identified and that records are protected against unauthorized addition, deletion, alteration, use and concealment.'  <i>ISO 15489-1, 7.2.2 Authenticity - p.7</i></p>

[\[back to top\]](#)

<p style="text-align: center;"><b>COMPLIANT</b></p> <p style="text-align: center;"><b>NOT COMPLIANT</b></p>	<p><b>3.5 The system must be supported by a digital preservation plan that anticipates and establishes contingencies for technological obsolescence at the level of storage media, data formats, application software and hardware.</b></p>
<p style="text-align: center;"><b>ANALYSIS COMMENTS</b></p>	
<p style="text-align: center;"><b>REQUIREMENT CITATIONS</b></p>	<p>'The storage of records in electronic form necessitates the use of additional storage plans and strategies to prevent their loss.' <i>ISO 15489-2, 8.3.5 Conversion and migration - p.19</i></p> <p>'Organizations should have policies and guidelines for converting or migrating records from one records system to another.' <i>ISO 15489-1, 9.6 Storage and handling - p.14</i></p> <p>'Records of continuing value, irrespective of format, require higher quality storage and handling to preserve them for as long as that value exists.' <i>ISO 15489-2, 4.3.9.2 Continuing Retention - p.20</i></p> <p>'Records identified for continuing retention need to be stored in environments conducive to their long-term preservation.' <i>ISO 15489-2, 4.3.9.2 Continuing Retention - p.20</i></p> <p>'RMAs shall manage and preserve any record in any supported repository, regardless of its format or structure, so that, when retrieved, it can be reproduced, viewed, and manipulated in the same manner as the original.' <i>DoD 5015.2 (v.2, 2002), C.2.2.5 Storing Records - C2.2.5.3.</i></p> <p><b><u>Implementation Considerations</u></b></p> <p>'Preservation strategies can include copying, conversion and migration of records.</p> <p>a) Copying is the production of an identical copy within the same type of medium (paper/microfilm/electronic) for example, from paper to paper, microfilm to microfilm or the production of backup copies of electronic records (which can also be made on a different kind of electronic medium).</p> <p>b) Conversion involves a change of the format of the record but ensures that the record retains the identical primary information (content). Examples include microfilming of paper records, imaging, change of character sets.</p> <p>c) Migration involves a set of organized tasks designed to periodically transfer digital material from one hardware/software configuration to another, or from one generation of technology to another. The purpose of</p>

	<p>migration is to preserve the integrity of the records and to retain the ability for clients to retrieve, display and otherwise use them. Migration may occur when hardware and/or software becomes obsolete or may be used to move electronic records from one file format to another.'</p> <p><i>ISO 15489-2, 4.3.9.2 Continuing Retention - P.20</i></p> <p>'The organization may meet this [preservation] requirement by:</p> <p>C2.2.10.3.1. Maintaining the hardware and software used to create or capture the record.</p> <p>C2.2.10.3.2. Maintaining hardware and software capable of viewing the record in its native format.</p> <p>C2.2.10.3.3. Ensuring backward compatibility when hardware and software is updated, or:</p> <p>C2.2.10.3.4. Migrating the record to a new format before the old format becomes obsolete. Any migration shall be pre-planned and controlled to ensure continued reliability of the record.'</p> <p><i>DoD 5015.2 (v.2, 2002), C2.2.10. Additional Baseline Requirements - C.2.2.10.3</i></p>
--	--

[\[back to top\]](#)

<b>COMPLIANT</b>	<b>3.6 The system must document all data format and media migrations that are carried out on the records in their metadata profiles as part of their preservation history.</b>
<b>NOT COMPLIANT</b>	
<b>ANALYSIS COMMENTS</b>	
<b>REQUIREMENT CITATIONS</b>	<p>'Systems for electronic records should be designed so that records will remain accessible, authentic, reliable and useable through any kind of system change, for the entire period of their retention. This may include migration to different software, representation in emulation formats or any other future ways of re-presenting records. <i>Where such processes occur, evidence of these should be kept, along with details of any variation in records design and format.'</i></p> <p><i>ISO 15489-1, 9.6 Storage and handling - p.14</i></p>

[\[back to top\]](#)

## 4. ACCESS

	<p>'Records systems should provide timely and efficient access to, and retrieval of, records needed in the continuing conduct of business and to satisfy related accountability requirements.'</p> <p><i>ISO 15489-1, 8.3.6 Access, retrieval and use - p.10</i></p> <p>'RMAs shall support simultaneous multiple-user access to all components of the RMA, the metadata, and the records.'</p> <p><i>DoD 5015.2 (v.2, 2002), C2.2.7. Access Controls - C2.2.7.5.</i></p>
--	---

[\[back to top\]](#)

<b>COMPLIANT</b>	<b>4.1 The system must provide the ability to search for, retrieve and display records.</b>
<b>NOT COMPLIANT</b>	
<b>ANALYSIS COMMENTS</b>	
<b>REQUIREMENT CITATIONS</b>	<p>'RMAs shall allow users to browse the records stored in the file plan based on their user access permissions.'</p> <p><i>DoD 5015.2 (v.2, 2002), C2.2.6.8. Searching for and Retrieving Records - C2.2.6.8.1.</i></p> <p>'RMAs shall allow searches using any combination of the record and/or folder metadata elements.'</p> <p><i>DoD 5015.2 (v.2, 2002), C2.2.6.8. Searching for and Retrieving Records - C2.2.6.8.2.</i></p> <p>'RMAs shall provide at least one portal that provides access to all associated repositories and databases storing electronic records and their metadata.'</p> <p><i>DoD 5015.2 (v.2, 2002), C2.2.5. Storing Records - C2.2.5.1</i></p> <p><b><u>Implementation Considerations</u></b></p> <p>'RMAs shall allow the user to specify partial matches and shall allow designation of "wild card" fields or characters.'</p>

*DoD 5015.2 (v.2, 2002), C2.2.6.8. Searching for and Retrieving Records - C2.2.6.8.3.*

'RMAs shall allow searches using Boolean and relational operators: "and," "and not," "or," "greater than" (>), "less than" (<), "equal to" (=), and "not equal to" (<>), and provide a mechanism to override the default (standard) order of precedence.'

*DoD 5015.2 (v.2, 2002), C2.2.6.8. Searching for and Retrieving Records - C2.2.6.8.4.*

'RMAs shall present the user a list of records and/or folders meeting the retrieval criteria, or notify the user if there are no records and/or folders meeting the retrieval criteria. RMAs shall allow the user to select and order the columns presented in the search results list for viewing, transmitting, printing, etc.'

*DoD 5015.2 (v.2, 2002), C2.2.6.8. Searching for and Retrieving Records - C2.2.6.8.5.*

'RMAs shall allow users the ability to search for null or undefined values.'

*DoD 5015.2 (v.2, 2002), C2.2.6.8. Searching for and Retrieving Records - C2.2.6.8.6.*

'RMAs shall allow the user to abort a search.'

*DoD 5015.2 (v.2, 2002), C2.2.6.8. Searching for and Retrieving Records - C2.2.6.8.11.*

'RMAs shall provide to the user's workspace (filename, location, or path name specified by the user) copies of electronic records, selected from the list of records meeting the retrieval criteria, in the format in which they were provided to the RMA

*DoD 5015.2 (v.2, 2002), C2.2.6.8. Searching for and Retrieving Records - C2.2.6.8.7.*

'RMAs shall allow users to select any number of records, and their metadata, for retrieval from the search results list.'

*DoD 5015.2 (v.2, 2002), C2.2.6.8. Searching for and Retrieving Records - C2.2.6.8.10.*

' When the user selects a record for retrieval, RMAs shall present a list of available versions, defaulting to the latest version of the record for retrieval, but allow the user to select and retrieve any version.'

*DoD 5015.2 (v.2, 2002), C2.2.6.8. Searching for and Retrieving Records - C2.2.6.8.9.*

'RMAs shall provide the capability for filed e-mail records to be retrieved back into a compatible e-mail application for viewing, forwarding, replying, and any other action within the capability of the e-mail application.'

*DoD 5015.2 (v.2, 2002), C2.2.6.8. Searching for and Retrieving Records - C2.2.6.8.8.*

[\[back to top\]](#)

<b>COMPLIANT</b>	<b>4.2 The system must enforce user access and security restrictions.</b>
<b>NOT COMPLIANT</b>	
<b>ANALYSIS COMMENTS</b>	
<b>REQUIREMENT CITATIONS</b>	<p>'Systems should include and apply controls on access to ensure that the integrity of the records is not compromised.' <i>ISO 15489-1, 8.3.6 Access, retrieval and use - p.10</i></p> <p>'Storage conditions and handling processes should be designed to protect records from unauthorized access, loss or destruction, and from theft and disaster.' <i>ISO 15489-1, 9.6 Storage and handling - p.14</i></p> <p>'RMAs shall allow only authorized individuals to move or delete records from the repository.' <i>DoD 5015.2 (v.2, 2002), C2.2.5. Storing Records. - C2.2.5.4.</i></p> <p>'The RMA, in conjunction with its operating environment, shall use identification and authentication measures that allow only authorized persons access to the RMA.' <i>DoD 5015.2 (v.2, 2002), C2.2.7. Access Controls - C2.2.7.1.</i></p> <p>'Managing the access process involves ensuring that:</p> <ul style="list-style-type: none"> <li>a) records are categorized according to their access status at a particular time,</li> <li>b) records are only released to those who are authorized to see them,</li> <li>c) encrypted records can be read as and when required and authorized,</li> <li>d) records processes and transactions are only undertaken by those authorized to perform them, and</li> <li>e) parts of the organization with responsibility for particular business functions specify access permissions to records relating to their area of responsibility.'</li> </ul> <p><i>ISO 15489-1, 9.7 Access - p.15</i></p> <p><b><u>Implementation Considerations</u></b></p> <p>'The degree of control of access and recording of use depends on the nature of the business and the records they generate. For example, mandatory privacy protection measures in many jurisdictions require that the use of records holding personal' <i>ISO 15489-2, 4.3.8 Use and tracking - p.19</i></p>

	<p>'RMAs shall provide the capability to define different groups of users with different access privileges. RMAs shall control access to file plan components, record folders, and records based on group membership as well as user account information. At a minimum, access shall be restricted to appropriate portions of the file plan for purposes of filing and/or searching/retrieving.'</p> <p><i>DoD 5015.2 (v.2, 2002), C2.2.7. Access Controls - C2.2.7.3</i></p> <p>'At a minimum, the RMA will implement identification and authentication measures that require the following:</p> <p>C2.2.7.1.1. Userid.</p> <p>C2.2.7.1.2. Password. (RMAs shall provide the capability for authorized users to define the minimum length of the Password field.)</p> <p>C2.2.7.1.3. Alternative methods, such as Biometrics, Common Access Cards (CAC), or Public Key Infrastructure (PKI), in lieu</p> <p><i>DoD 5015.2 (v.2, 2002), C2.2.7. Access Controls - C2.2.7.1</i></p> <p>'If the RMA provides a web user interface, it shall provide 128-bit encryption and be PKI-enabled, as well as provide all the mandatory access controls.'</p> <p><i>DoD 5015.2 (v.2, 2002), C2.2.7. Access Controls - C2.2.7.4.</i></p>
--	---

[\[back to top\]](#)

5. TRACKING	
	<p>'Tracking of the movement and use of records within a records system is required to</p> <ul style="list-style-type: none"> <li>a) identify outstanding action required,</li> <li>b) enable retrieval of a record,</li> <li>c) prevent loss of records,</li> <li>d) monitor usage for systems maintenance and security, and maintain an auditable trail of records transactions (i.e. capture or registration, classification, indexing, storage, access and use, migration and disposition), and</li> <li>e) maintain capacity to identify the operational origins of individual records where systems have been amalgamated or migrated'</li> </ul> <p><i>ISO 15489-1, 9.8 Tracking - p.15</i></p> <p>'The tracking of records usage within records systems is a security measure for organizations. It ensures that only those users with appropriate permissions are performing records tasks for which they have been authorized.'</p> <p><i>ISO 15489-2, 4.3.8 Use and tracking - p.19</i></p>

[\[back to top\]](#)

<b>COMPLIANT</b>	<b>5.1 The system must track the current location and custody of records, including checked out records or copies of records.</b>
<b>NOT COMPLIANT</b>	
<b>ANALYSIS COMMENTS</b>	
<b>REQUIREMENT CITATIONS</b>	<p>'The movement of records should be documented to ensure that items can always be located when required.'  <i>ISO 15489-1, 9.8.3 Location tracking - p.15</i></p> <p>'The system should track the issue, transfer between persons and return of records to their home location or storage as well as their disposition or transfer to any other authorized external organization including an archives authority.'  <i>ISO 15489-1, 9.8.3 Location tracking - p.15</i></p> <p><b><u>Implementation Considerations</u></b></p> <p>'Tracking mechanisms may record the item identifier, the title, the person or unit having possession of the item and the time/date of movement.'  <i>ISO 15489-1, 9.8.3 Location tracking - p.15</i></p> <p>'Systems for monitoring use and/or movement of records range from</p> <ul style="list-style-type: none"> <li>- physical card-based movement-recording systems to</li> <li>- bar-coding technology to</li> <li>- electronic records systems where viewing a record is automatically captured as a system transaction.'</li> </ul> <p><i>ISO 15489-2, 4.3.8 Use and tracking - p.19</i></p> <p>'Tracking systems have to meet the test of locating any record within an appropriate time period and ensuring that all movements are traceable.'  <i>ISO 15489-2, 4.3.8 Use and tracking - p.19</i></p>

[\[back to top\]](#)

<p style="text-align: center;"><b>COMPLIANT</b></p> <p style="text-align: center;"><b>NOT COMPLIANT</b></p>	<p><b>5.2 The system must maintain secured audit logs on the access and use of records.</b></p>
<p style="text-align: center;"><b>ANALYSIS COMMENTS</b></p>	
<p style="text-align: center;"><b>REQUIREMENT CITATIONS</b></p>	<p>'[Records systems] should provide and maintain audit trails or other methods to demonstrate that records were effectively protected from unauthorized use, alteration or destruction.'  <i>ISO 15489-1, 8.3.6 Access, retrieval and use - p.10</i></p> <p>'The RMA, in conjunction with its operating environment, shall provide an audit capability to log the actions, date, time, unique object identifier(s) and user identifier(s) for actions performed on the following RMA objects:  C2.2.8.1.1. User Accounts.  C2.2.8.1.2. User Groups.  C2.2.8.1.3. Records.  C2.2.8.1.4. Associated metadata elements.  C2.2.8.1.5. File plan components.</p> <p>These actions include retrieving, creating, deleting, searching, and editing actions.'  <i>DoD 5015.2 (v.2, 2002), C2.2.8. System Audits - C2.2.8.1.</i></p> <p>' The RMA, in conjunction with its operating environment, shall provide audit analysis functionality whereby an authorized individual can set up specialized reports to:  C2.2.8.3.1. Determine what level of access a user has and to track a user's actions.  C2.2.8.3.2. Facilitate reconstruction, review, and examination of the events surrounding or leading to mishandling of records, possible compromise of sensitive information, or denial of service.'  <i>DoD 5015.2 (v.2, 2002), C2.2.8. System Audits - C2.2.8.3.</i></p> <p>'Records systems should contain complete and accurate representations of all transactions that occur in relation to a particular record.  - These include the processes associated with individual records.  - Such details may be documented as part of the metadata embedded in, attached to, or associated with, a specific record.'  <i>ISO 15489-1, 8.3.2 Documenting record transactions - p.9</i></p> <p>'The tracking of records usage within records systems is a security measure for organizations. It ensures that only those users with appropriate permissions are performing records tasks for which they have been authorized.'</p>

	<p style="text-align: center;"><i>ISO 15489-2, 4.3.8 Use and tracking - p.19</i></p> <p><b><u>Implementation Considerations</u></b></p> <p>'The RMA, in conjunction with its operating environment, shall not allow audit logs to be edited.'  <i>DoD 5015.2 (v.2, 2002), C2.2.8. System Audits - C2.2.8.6.</i></p> <p>'Tracking systems have to meet the test of locating any record within an appropriate time period and ensuring that all movements are traceable.'  <i>ISO 15489-2, 4.3.8 Use and tracking - p.19</i></p> <p>'RMAs shall provide the capability to file the audit data as a record.'  <i>DoD 5015.2 (v.2, 2002), C2.2.8. System Audits - C2.2.8.4.</i></p> <p>'The RMA, in conjunction with its operating environment, shall allow only authorized individuals to export and/or backup and remove audit files from the system.'  <i>DoD 5015.2 (v.2, 2002), C2.2.8. System Audits - C2.2.8.5.</i></p>
--	--

[\[back to top\]](#)

<b>COMPLIANT</b>	<b>5.3 The system must establish version control and differentiate original records from drafts and copies.</b>
<b>NOT COMPLIANT</b>	
<b>ANALYSIS COMMENTS</b>	
<b>REQUIREMENT CITATIONS</b>	<p>'An organization may determine that RMAs should have the capability to manage working and draft versions of documents and other potential record materials as they are being developed.'  <i>DoD 5015.2 (v.2, 2002), C3.2. Other Useful RMA Features - C3.2.11.</i></p> <p>'Records management policies and procedures should specify</p> <ul style="list-style-type: none"> <li>-what additions or annotations may be made to a record after it is created,</li> <li>-under what circumstances additions or annotations may be authorized, and who is authorized to make them.</li> <li>-Any authorized annotation, addition or deletion to a record should be explicitly indicated and traceable.'</li> </ul>

*ISO 15489-1, 7.2.4 Integrity - p.7*

**Implementation Considerations**

' When the user selects a record for retrieval, RMAs shall present a list of available versions, defaulting to the latest version of the record for retrieval, but allow the user to select and retrieve any version.'

*DoD 5015.2 (v.2, 2002), C2.2.6.8. Searching for and Retrieving Records - C2.2.6.8.9.*

' When the user selects a record for retrieval, RMAs shall present a list of available versions, defaulting to the latest version of the record for retrieval, but allow the user to select and retrieve any version.'

*DoD 5015.2 (v.2, 2002), C2.2.6.8. Searching for and Retrieving Records - C2.2.6.8.9.*

[\[back to top\]](#)

## 6. DISPOSITION

'Disposition authorities that govern the removal of records from operational systems should be applied to records on a systematic and routine basis, in the course of normal business activity.'

*ISO 15489-1, 9.9 Implementing disposition - p.16*

'Records retention should be managed to meet the current and future needs of internal and external stakeholders by following regulations of the appropriate archival authority where applicable.'

*ISO 15489-1, 9.2 Determining how long to retain records - p.12*

'Statutory or other regulatory requirements may demand minimum retention periods or submission to an authorizing body such as an archival authority or auditors for any necessary approval [of the records disposition authority].'

*ISO 15489-1, 9.2 Determining how long to retain records - p.11*

'RMAs shall provide the capability for only authorized individuals to view, create, edit, and delete disposition schedule components of record categories.'

*DoD 5015.2 (v.2, 2002), C2.2.2. Scheduling Records - C2.2.2.1.*

'RMAs shall provide the capability for only authorized individuals to define the cutoff criteria and, for each life-cycle phase, the following disposition components for a record category:

C2.2.2.3.1. Retention Period (e.g., fiscal year).

C2.2.2.3.2. Disposition Action (interim transfer, accession, permanent, or destroy).

C2.2.2.3.3. Interim Transfer or Accession Location (if applicable).'

*DoD 5015.2 (v.2, 2002), C2.2.2. Scheduling Records - C2.2.2.3.*

'Records systems should be capable of facilitating and implementing decisions on the retention or disposition of records.

- It should be possible for these decisions to be made at any time in the existence of records, including during the design stage of records systems.

- It should also be possible, where appropriate, for disposition to be activated automatically.'

*ISO 15489-1, 8.3.7 Retention and disposition - p.10*

'Records retention should be managed to meet current and future business needs by:

- retaining information concerning past and present decisions and activities as part of the corporate memory to inform decisions and activities in the present and in the future,

- retaining evidence of past and present activities to meet accountability obligations,

- eliminating, as early as possible and in an authorized, systematic manner, records which are no longer required, and

- retaining the context of the record which will enable future users to judge the authenticity and reliability of records, even in cases where the records systems in which they are retained have been closed or have undergone significant changes.'

*ISO 15489-1, 9.2 Determining how long to retain records - p.12*

'[A records disposition authority is] a formally approved schedule of classes of records, retention periods and appropriate disposition actions that is submitted for approval by an external authority (on records disposition).'

*ISO 15489-2, 4.2.4 Records disposition authority - p.10*

'All decisions on which records should be captured and how long records should be maintained should be clearly documented and retained. Decisions may be presented as a disposition authority.'

*ISO 15489-1, 9.10 Documenting records management processes - p.16*

'Disposition action may encompass:

- a) immediate physical destruction, including overwriting and deletion,
- b) retention for a further period within the business unit,
- c) transfer to an appropriate storage area or medium under organizational control,
- d) transfer to another organization that has assumed responsibility for the business activity through restructure, sale or privatization,
- e) transfer to a storage area managed on behalf of the organization by an independent provider with whom appropriate contractual arrangements have been established,
- f) transfer of responsibility for management to an appropriate authority while physical storage of the record is retained by the creating organization,
- g) transfer to an organizational archive, or

*ISO 15489-1, 9.9 Implementing disposition - p.16*

'Initially, such decisions [on how long to retain records] should involve the unit administering the specific business activity, the designated records manager and others as required, in compliance with the external and internal records management policies or standards and the requirements for records associated with the specific business activity.'

*ISO 15489-1, 4.2.4.3 Determining how long to retain records - p.11*

'Records identified for continuing retention are likely to be those which:

- provide evidence and information about the organization's policies and actions,
- provide evidence and information about the organization's interaction with the client community it serves,
- document the rights and obligations of individuals and organizations,
- contribute to the building of an organization's memory for scientific, cultural or historical purposes, and
- contain evidence and information about activities of interest to internal and external stakeholders.'

*ISO 15489-1, 9.2 Determining how long to retain records - p.12*

#### **Implementation Considerations**

'In electronic records systems, the determinations about capture and retention should be considered in system design at the outset

*ISO 15489-2, 4.2.4 Records disposition authority - p.10*

'Determining what records should be captured and how long they should be kept is most effectively undertaken in a systematic way and according to laws and regulations (which may be country-specific, specific to different types of organizations or industries or related to certain products). Instruments to standardize the decision-making may range from guidelines identifying what documents should be destroyed or captured into records systems to a formally approved schedule of classes of records, retention periods and appropriate disposition actions that is submitted for approval by an external authority (records disposition  
*ISO 15489-2, 4.2.4 Records disposition authority - p.8*

'Decisions on records capture as part of a system design process are best undertaken in conjunction with the business unit responsible for the activity and systems.'  
*ISO 15489-2, 4.2.4.2 Determining documents to be captured into a records system - p.11*

'The rights and interests of all stakeholders should be considered when determining how long records need to be maintained. The decisions should not be made intentionally to circumvent any rights of access.'  
*ISO 15489-1, 4.2.4.3 Determining how long to retain records - p.11*

'Consider the broad range of uses of the record. Steps in this process include identifying other stakeholders, for example, archives or external users, with enforceable or legitimate interests in preserving the record longer than the internal users of the organization; assessing the risks associated with destroying the record, once routine, internal use of the record has finished; considering what records and actions to preserve them would be required by the organization to ensure business continuity in the event of loss or damage to the records; assessing financial, political, social or other positive gains from maintaining the record after organizational use has been completed; and, analysing the balance between the costs and non-financial gains of records retention to decide how long records are maintained after organizational needs have been met.'  
*ISO 15489-2, 4.2.4.3 Determining how long to retain records - p.11-12*

'RMAs shall provide the capability for defining multiple phases (e.g., transfer to inactive on-site storage, transfer to off-site storage) within a disposition schedule.'  
*DoD 5015.2 (v.2, 2002), C2.2.2. Scheduling Records - C2.2.2.2.*

[\[back to top\]](#)

<b>COMPLIANT</b>	<b>6.1 The system must be able to calculate the retention period for records and trigger the appropriate disposition event when the retention period expires.</b>
<b>NOT COMPLIANT</b>	
<b>ANALYSIS COMMENTS</b>	
<b>REQUIREMENT CITATIONS</b>	<p>'Any records created or captured need to have a retention period assigned, so it is clear how long they should be maintained.'  <i>ISO 15489-2, 4.2.4.2 Determining documents to be captured into a records system - p.11</i></p> <p>'RMAs shall provide the capability to automatically calculate the complete life cycle, including intermediate phases, of record folders and records not in folders.'  <i>DoD 5015.2 (v.2, 2002), C2.2.2. Scheduling Records - C2.2.2.5.</i></p> <p>'RMAs shall, as a minimum, be capable of scheduling and rescheduling each of the following three types of cutoff and disposition instructions.  C2.2.2.4.1. Time Dispositions, where records are eligible for disposition immediately after the conclusion of a fixed period of time following user-defined cutoff (e.g., days, months, years).  C2.2.2.4.2. Event Dispositions, where records are eligible for disposition immediately after a specified event takes place (i.e., event acts as cutoff and there is no retention period).  C2.2.2.4.3. Time -Event Dispositions, where the timed retention periods are triggered after a specified event takes place (i.e., event makes the record folder eligible for closing and/or cutoff and there is a retention period).'</p> <p><i>DoD 5015.2 (v.2, 2002), C2.2.2. Scheduling Records - C2.2.2.4.</i></p> <p>'Disposition action may encompass:  a) immediate physical destruction, including overwriting and deletion,  b) retention for a further period within the business unit,  c) transfer to an appropriate storage area or medium under organizational control,  d) transfer to another organization that has assumed responsibility for the business activity through restructure, sale or privatization,  e) transfer to a storage area managed on behalf of the organization by an independent provider with whom appropriate contractual arrangements have been established,  f) transfer of responsibility for management to an appropriate authority while physical storage of the record is retained by the</p>

creating organization,  
g) transfer to an organizational archive, or  
*ISO 15489-1, 9.9 Implementing disposition - p.16*

### **Implementation Considerations**

'Records with similar disposition dates and triggering actions should be readily identifiable from the records system. For example, paper-based records with the same disposition dates and triggering actions can be stored physically together.'  
*ISO 15489-2, 4.3.9.1 Implement Disposition - p.20*

'Similar retention periods and disposition action are determined for groups of records performing or recording similar activities within the system. Retention periods should be stated clearly and disposition triggers clearly identified. For example: 'destroy x years after audit' or 'transfer to the archives x years after last transaction completed'.'  
*ISO 15489-2, 4.2.4.3 Determining how long to retain records - p.11-12*

'RMAs shall provide for sorting, viewing, saving, and printing list(s) of record folders and/or records (regardless of media) based on any combination of the following:

- C2.2.6.1.1.1. Disposition Action Date.
- C2.2.6.1.1.2. Disposition Action.
- C2.2.6.1.1.3. Location.
- C2.2.6.1.1.4. Transfer or Accession Location.
- C2.2.6.1.1.5. Vital Records Review and Update Cycle Period or Date.
- C2.2.6.1.1.6. Record Category Identifier.
- C2.2.6.1.1.7. Folder Unique Identifier.
- C2.2.6.1.1.8. User Definable Fields.'

*DoD 5015.2 (v.2, 2002), C2.2.6. Retention and Vital Records Management - C2.2.6.1.1.*

'RMAs shall identify and present the record folders and records, including record metadata, that are eligible for destruction, as a result of reaching that phase in their life cycle. Records assigned more than one disposition must be retained and linked to the Record Folder (Category) with the longest retention period. Links to Record Folders (Categories) with shorter retention periods should be removed as they become due.'

*DoD 5015.2 (v.2, 2002), C2.2.6.6. Destroying Records - C2.2.6.6.1.*

'RMAs shall identify and present those record folders and records eligible for interim transfer and/or accession.'

*DoD 5015.2 (v.2, 2002), C2.2.6.5. Transferring Records - C2.2.6.5.1.*

'RMAs shall be capable of implementing cutoff instructions for scheduled and unscheduled record folders. RMAs shall identify record folders eligible for cutoff, and present them only to the authorized individual for cutoff approval. The cutting off of a folder shall start the first phase of its life cycle controlled by the records schedule.'

*DoD 5015.2 (v.2, 2002), C2.2.6. Retention and Vital Records Management - C2.2.6.3.1.*

'RMAs shall provide authorized individuals with the capability to indicate when the specified event has occurred for records and record folders with event- and time-event-driven dispositions.'

*DoD 5015.2 (v.2, 2002), C2.2.6. Retention and Vital Records Management - C2.2.6.1.4*

'RMAs shall provide a capability for authorized individuals to close record folders to further filing after the specified event occurs.'

*DoD 5015.2 (v.2, 2002), C2.2.6. Retention and Vital Records Management - C2.2.6.2.1.*

'RMAs shall provide for sorting, viewing, saving, and printing lists and partial lists of record folders and/or records that have no assigned disposition.'

*DoD 5015.2 (v.2, 2002), C2.2.6. Retention and Vital Records Management - C2.2.6.1.5*

'RMAs shall provide the capability only to authorized individuals to add records to a previously closed record folder or to reopen a previously closed record folder for additional public filing.'

*DoD 5015.2 (v.2, 2002), C2.2.6. Retention and Vital Records Management - C2.2.6.2.2.*

'The use history of records due for disposition action needs to be reviewed to confirm or amend the disposition status.'

*ISO 15489-2, 4.3.9.1 Implement Disposition - p.20*

'RMAs shall provide the capability for only authorized individuals to extend or suspend (freeze) the retention period of record folders or records beyond their scheduled disposition.

C2.2.6.4.3. RMAs shall identify record folders and/or records that have been frozen and provide authorized individuals with the capability to unfreeze them.'

*DoD 5015.2 (v.2, 2002), C2.2.6. Retention and Vital Records Management - C2.2.6.4.1.*

C2.2.2.7. The RMA shall provide recalculation of the record life cycle based on changes to any life-cycle date and set the filing status (i.e., open, closed) of the folder according to the business rules associated with date change(s).'

*DoD 5015.2 (v.2, 2002), C2.2.2. Scheduling Records - C2.2.2.6.*

[\[back to top\]](#)

<b>COMPLIANT</b>	
<b>NOT COMPLIANT</b>	<p><b>6.2 The system must be able to preserve those records that require long-term or permanent retention in accordance with a digital preservation plan (see Requirement 3.5) or transfer them to a storage repository that meets long-term preservation requirements.</b></p>
<b>ANALYSIS COMMENTS</b>	
<b>REQUIREMENT CITATIONS</b>	<p>'Disposition authorities that govern the removal of records from operational systems should be applied to records on a systematic and routine basis, in the course of normal business activity.'  <i>ISO 15489-1, 9.9 Implementing disposition - p.16</i></p> <p>'RMAs shall, for records approved for interim transfer or accession and that are stored in the RMA's supported repository(ies), copy the pertinent records and associated metadata of the records and their folders to a user-specified filename, path, or device.'  <i>DoD 5015.2 (v.2, 2002), C2.2.6.5. Transferring Records - C2.2.6.5.2.</i></p> <p>'A transfer of ownership or custody of records to another organization may include: transfer to other organizations with responsibilities for the records, transfer to outsourced or contractor organizations, transfer to a storage facility, or transfer to  <i>ISO 15489-2, 4.3.9.4 Transfer of custody or ownership of records - p.21</i></p> <p>'Where records are removed from the immediate physical environment of the business unit into other physical areas controlled by the organization, the continuing responsibility for authorizing the destruction or further disposition action is retained by that  <i>ISO 15489-2, 4.3.9.2 Continuing Retention - p.20</i></p> <p>'In some countries, the disposition authorities may prescribe permanent preservation, either within the organization or in a separate archives institution.'  <i>ISO 15489-2, 4.2.4 Records disposition authority - p.10</i></p> <p><b><u>Implementation Considerations</u></b></p> <p>'No disposition action should take place without the assurance that the record is no longer required, that no work is outstanding and that no litigation or investigation is current or pending which would involve relying on the record as evidence.'  <i>ISO 15489-1, 9.9 Implementing disposition - p.16</i></p>

'If electronic records are transferred, such issues as the following need to be considered: hardware and software compatibility; metadata (control and contextual information); data documentation (technical information on data processing and data structure); licensing agreements; and standards.'

*ISO 15489-2, 4.3.9.4 Transfer of custody or ownership of records - p.21*

'Where records are transferred to an external storage provider or an external archives authority, whether as a result of implementing disposition action or for other reasons, documentation outlining continuing obligations to maintain the records and manage them appropriately, safeguarding their retention or disposition and accessibility, are formally established by agreement between the custodian(s) and the transferring party.'

*ISO 15489-2, 4.3.9.2 Continuing Retention - p.20*

'In such cases where records are being removed from the control or ownership of the organization (for example, through privatization of government agencies), consent of the responsible archival authority may be required.'

*ISO 15489-2, 4.3.9.4 Transfer of custody or ownership of records - p.21*

'A key element in dealing with the transfer of ownership of records is the determination of accountability for records. Examples of questions in this context include the following:

- a) Have the operational and administrative needs for transfer of the records been authoritatively established?
- b) Have the issues of authority and accountability for records been addressed?
- c) Has the impact on the transferring institution's records been taken into account?
- d) Have the ongoing legislative, policy and regulatory obligations been fulfilled?'

*ISO 15489-2, 4.3.9.4 Transfer of custody or ownership of records - p.21*

'RMAs shall, for records approved for interim transfer or accession, provide the capability for only authorized individuals to delete the records and/or related metadata after successful transfer has been confirmed. RMAs shall provide the capability to allow the organization to retain the metadata for records that were transferred or accessioned.'

*DoD 5015.2 (v.2, 2002), C2.2.6.5. Transferring Records - C2.2.6.5.4.*

[\[back to top\]](#)

<b>COMPLIANT</b>	<b>6.3 The system must be able to completely and reliably expunge those records that have been assigned 'destruction' as their final disposition action (including any backup, reference or source copies).</b>
<b>NOT COMPLIANT</b>	
<b>ANALYSIS COMMENTS</b>	
<b>REQUIREMENT CITATIONS</b>	<p>'All copies of records that are authorized for destruction, including security copies, preservation copies and backup copies, should be destroyed.'  <i>ISO 15489-1, 9.9 Implementing disposition - p.16</i></p> <p>'The using organization shall schedule the backup copies and recycle or destroy the medium in accordance with the disposition'  <i>DoD 5015.2 (v.2, 2002), C2.2.10. Additional Baseline Requirements. - C2.2.10.6.</i></p> <p><b><u>Implementation Considerations</u></b></p> <p>'No disposition action should take place without the assurance that the record is no longer required, that no work is outstanding and that no litigation or investigation is current or pending which would involve relying on the record as evidence.'  <i>ISO 15489-1, 9.9 Implementing disposition - p.16</i></p> <p>'RMAs shall, for records approved for destruction, present a second confirmation requiring authorized individuals to confirm the delete command, before the destruction operation is executed.'  <i>DoD 5015.2 (v.2, 2002), C2.2.6.6. Destroying Records - C2.2.6.6.2.</i></p> <p>'Destruction should always be authorized.'  <i>ISO 15489-1, 9.9 Implementing disposition - p.16</i></p> <p>'RMAs shall restrict the records destruction commands to authorized individuals.'  <i>DoD 5015.2 (v.2, 2002), C2.2.6.6. Destroying Records - C2.2.6.6.5.</i></p> <p>'Records destruction should be carried out in a way that preserves the confidentiality of any information they contain.'  <i>ISO 15489-1, 9.9 Implementing disposition - p.16</i></p> <p>'Physical destruction of records is carried out by methods appropriate to their level of confidentiality.'  <i>ISO 15489-2, 4.3.9.3 Physical destruction - p.21</i></p> <p>'RMAs shall delete electronic records approved for destruction in a manner such that the records cannot be physically</p>

	<p><i>DoD 5015.2 (v.2, 2002), C2.2.6.6. Destroying Records - C2.2.6.6.3.</i></p> <p>'Records in electronic form can also be destroyed by reformatting or rewriting if it can be guaranteed that the reformatting cannot be reversed. Delete-instructions are not sufficient to ensure that all system pointers to the data incorporated in the system software have also been destroyed. Backups containing generations of system data also need to be reformatted or rewritten before effective destruction of information in electronic form is complete. Physical destruction of storage media is an appropriate alternative, especially if deletion, reformatting or rewriting are either not applicable or are unsafe methods for destroying digital information (for instance, information stored on WORM [Write Once Read Many] media).'</p> <p><i>ISO 15489-2, 4.3.9.3 Physical destruction - p.21</i></p> <p>'Destruction can be undertaken by third parties contracted for the task.'</p> <p><i>ISO 15489-2, 4.3.9.3 Physical Destruction - p.21</i></p>
--	--

[\[back to top\]](#)

<b>COMPLIANT</b>	<b>6.4 The system must document retention information and disposition events in the record's metadata profile.</b>
<b>NOT COMPLIANT</b>	
<b>ANALYSIS COMMENTS</b>	
<b>REQUIREMENT CITATIONS</b>	<p>'Other important [disposition] activities are maintaining an auditable record of disposition action.'</p> <p><i>ISO 15489-2, 4.3.9.1 Implement Disposition - p.20</i></p> <p>'RMAs shall provide documentation of transfer activities. This documentation shall be stored as records.'</p> <p><i>DoD 5015.2 (v.2, 2002), C2.2.6.5. Transferring Records - C2.2.6.5.5.</i></p> <p>'RMAs shall, for records approved for accession and that are not stored in an RMA supported repository, copy the associated metadata for the records and their folders to a user-specified filename, path, or device.'</p> <p><i>DoD 5015.2 (v.2, 2002), C2.2.6.5. Transferring Records - C2.2.6.5.3.</i></p> <p>'The organization may maintain an auditable trail documenting all destruction of records.'</p> <p><i>ISO 15489-2, 4.3.9.3 Physical Destruction - p.21</i></p>

'RMAs shall provide documentation of destruction activities. This documentation shall be stored as records.'

*DoD 5015.2 (v.2, 2002), C2.2.6.6. Destroying Records - C2.2.6.6.6.*

'RMAs shall provide a field for authorized individuals to enter the reason for freezing a record or record folder.'

C2.2.6.4.4. RMAs shall allow authorized individuals to search, update, and view the reason for freezing a record or record

*DoD 5015.2 (v.2, 2002), C2.2.6. Retention and Vital Records Management - C2.2.6.4.2.*

'Certificates of destruction are recommended for all destruction undertaken by third parties.'

*ISO 15489-2, 4.3.9.3 Physical Destruction - p.21*

[\[back to top\]](#)