A
Records Management Standards

ISO-15489

The goal of the ISO-15489 standard is to alert organizations to the importance of Records Management and to introduce them to a set of Records Management best practices. Organizations that adopt ISO-15489 best practices are able to achieve greater efficiencies, reduce costs, and increase profits.

ISO-15489 is a broad standard. Compared to the DoD 5015.2 and MoReq2 standards, ISO-15489 provides very little detail about how to actually implement a Records Management system. Instead, it focuses on describing a high-level framework for managing records.

ISO-15489 began in Australia in 1996 as the Australian Standard on Records Management (AS4390). The ISO version of this standard was first published in October 2001.

Elements of ISO-15489

ISO-15489 consists of two parts. The first part is the standard itself, and the second part is a document that includes guidelines for how best to comply with the standard.

The components of the standard, as described in part one, include:

- Policies and responsibilities
- Records Management requirements

- Design and implementation of a records system
- Records Management processes and controls
- Monitoring and auditing
- Training

More information about ISO-15489 is available directly from ISO: `http://www.iso.org/iso/catalogue_detail.htm?csnumber=31908`.

DoD 5015.2

In April 1997, the United States Department of Defence (DoD) released a document titled *Design Criteria Standard for Electronic Records Management Software Applications*. This standard for Records Management implementations has become the "Gold Standard" when judging the capabilities of Electronic Records Management Systems in the United States.

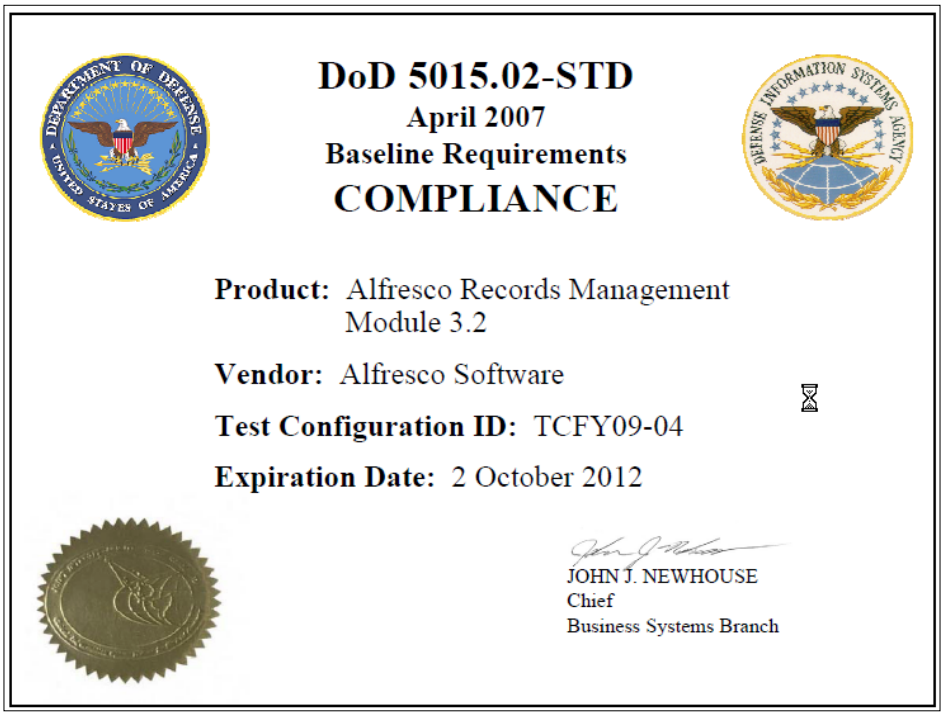
The standard is now often simply referred to as "5015.2", the internal DoD directive number associated with the document. Version 2 of the DoD 5015.2 standard was released in June, 2002 and it was updated again in 2007.

DoD 5015.2 was originally designed to be used only by the DoD, defense agencies, and the US military, but its use was later expanded to include other government agencies. The design of 5015.2 attempted to ensure compliance with US laws and regulations.

Despite its origins as a US-government-focused standard, many corporations and international governments have since adapted the standard for their own use.

Alfresco 5015.2-STD certification

Alfresco has achieved **Baseline Requirements** certification for the DoD 5015.2-STD:



DoD 5015.02-STD
April 2007
Baseline Requirements
COMPLIANCE

Product: Alfresco Records Management Module 3.2

Vendor: Alfresco Software

Test Configuration ID: TCFY09-04

Expiration Date: 2 October 2012

JOHN J. NEWHOUSE
Chief
Business Systems Branch

DoD 5015.2 product certification is a rigorous process costing tens of thousands of dollars that often takes as long as two weeks to complete. Testing is performed by the **Joint Interoperability Test Command** (**JITC**). Each test case required for certification is hand-tested by a member of the JITC, using the vendor's software.

Once a vendor's software has been tested and certified as compliant with 5015.2, the certification is posted on the JITC's website. Certification is valid for three years.

Government agencies that are required to purchase DoD 5015.2 certified software are limited to selecting software from the list of vendors included in the JITC list of certified products.

The number of vendors and products that have actually been certified for the DoD 5015.2 is fairly small. Many companies claim to have products that are "5015.2 compliant," but for whatever reason have not had their software certified.

Alfresco DoD 5015.2 certification matrix

The certification matrix achieved by Alfresco Records Management Module version 3.2 is as follows:

Item		Version
Server operating system	Red Hat Enterprise Linux (RHEL)	2.6.18
	MS Windows	2008 (SP2)
Workstation operating system	MS Windows	XP (SP3)
Database management system	MySQL	5.0.77
	Oracle	10.2
E-mail server	Zimbra	6.0.1 GA
E-mail client	MS Outlook	2007 (SP1)
Web servers	Tomcat	6.0.18
	JBoss AS	5.1.0 GA
Web browsers	MS Internet Explorer	7
	Firefox	3.5
Office automation	MS Office	2007 (SP1)
Repository/storage of the electronic content	Red Hat Enterprise Linux (RHEL)	2.6.18

The online 5015.2 certification can be found at `http://jitc.fhu.disa.mil/recmgt/alfresco/index.html`.

DoD 5015.2 metadata requirements

The DoD 5015.2 standard mandates that the following metadata properties be included.

File Plan components

- Record Category Name
- Record Category Identifier (must be unique)
- Record Category Description
- Disposition Instructions

- Disposition Authority
- Transfer or Accession to NARA indicator
- Vital Record Indicator
- Vital Record Review and Update Cycle (Mandatory if vital record indicator is set)
- Organizational Definable Fields

Record folder components

- Folder Name
- Folder Identifier (Must be unique)
- Location (mandatory for records not in the electronic repository)
- Vital Record Indicator
- Vital Record Review and Update Cycle (mandatory if the vital record indicator is set)
- Supplemental Marking List
- Organizational Definable Fields

Record metadata components

- Record Identifier (Must be unique)
- Subject or Title
- Date Filed
- Publication date
- Author or Originator
- Originating Organization
- Supplemental Marking List
- Media Type
- Format
- Addressee(s) (mandatory for correspondence)
- Other Addressee(s) (mandatory for correspondence)
- Location
- Organization-Defined Fields

DoD 5015.2 mandatory baseline requirements

What follows here is an overview of the mandatory requirements of the DoD 5015.2 April 17, 2007 specification. The DoD document is 118 pages and should be consulted for more detailed information.

Implementing File Plans

1. Must allow authorized individuals to create a record category containing a record category ID, record category name, and a record category description (C2.2.1.1).
2. Must allow authorized individuals to find and edit a record category (C2.2.1.1).
3. Must allow authorized individuals to delete a record category (C2.2.1.1).
4. Must allow authorized individuals to create a record subcategory of a record category (C2.2.1.1).
5. Must allow authorized individuals to be able to specify the items that appear in drop-down selection lists (C2.2.1.2).
6. Must allow authorized individuals to create which metadata properties are to be collected for the File Plan (C2.2.1.3).
7. Must allow authorized individuals to specify which metadata fields are mandatory (C2.2.1.4).
8. Must allow authorized individuals to create, edit, and delete a record folder, including their components and identifiers (C2.2.1.5).
9. Must be possible for authorized individuals to sort, view, save, and print the File Plan (C2.2.1.6).
10. Must ensure that File Plan identifiers are unique so that ambiguous references can't occur (C2.2.1.7).
11. Must allow authorized users the ability to create scripts that can perform actions like alerts and notifications (C2.2.1.9).
12. Must be able to sort the File Plan by a single or multiple fields (C2.2.1.10).

Scheduling records

1. Must allow authorized individuals to create, find, view, and edit the elements of the disposition schedule for record categories (C2.2.2.1).
2. Must support multiple editable steps for the disposition schedule (C2.2.2.2).
3. Must be able to define parallel or interdependent steps within the disposition schedule (C2.2.2.3).
4. Must allow authorized individuals to select cutoff to trigger the start of the disposition (C2.2.2.4).
5. Must be able to schedule dates for steps of the retention and disposition (C2.2.2.5).
6. Must allow authorized individuals to edit cutoff and other elements of the disposition schedule (C2.2.2.6).
7. Must allow authorized individuals to define the disposition schedule instruction information, retention period, disposition action, interim transfer, or accession location. (C2.2.2.3.1-3).
8. Must be able to schedule and reschedule cutoff and disposition instructions for the following:
   a. Time dispositions (C2.2.2.7.1)
   b. Event dispositions (C2.2.2.7.2)
   c. Time-Event dispositions (C2.2.2.7.2)
9. Must be able to name the events of the disposition and be able to support more than one, possibly triggering the disposition action (C2.2.2.8).
10. Must be able to automatically schedule dates for the record lifecycle, including intermediate dates on folders and records (C2.2.2.9).
11. Must allow authorized individuals to reschedule dispositions on folders and records if disposition instructions change (C2.2.2.10).
12. Must be able to recalculate the dates in the record lifecycle if business rules cause dates to need to be changed (C2.2.2.11).

Declaring and filing records

1. Must be able to associate a record with a folder (C2.2.3.1).
2. Must be able to associate a record with a category (C2.2.3.1).
3. Must include certain metadata properties standard for record objects as specified below (C2.2.3.2).
4. Must allow authorized individuals to create, edit, and delete metadata properties associated with records (C2.2.3.3).
5. Must allow authorized individuals to indicate which metadata properties are mandatory (C2.2.3.4).
6. Must be able to assign a unique record ID to a record (C2.2.3.5).
7. Must be able to create, view, and save record metadata (C2.2.3.6).
8. Must be able to print all or part of the record metadata (C2.2.3.6).
9. Must be able to prevent changes to records (C2.2.3.7).
10. Must not be able to edit metadata fields that are not editable (C2.2.3.8).
11. Must allow users a way to enter the data of metadata fields (C2.2.3.9).
12. Must ensure that required metadata fields are non-null (C2.2.3.9).
13. Must allow users to edit metadata fields prior to filing (C2.2.3.10).
14. Must enforce validation of date format for metadata (C2.2.3.11).
15. Must allow only authorized individuals to define and add metadata properties (C2.2.3.12).
16. Must be able to view, save, or print metadata for the File Plan, folders, and records (C2.2.3.13).
17. Must be able to limit the categories or folders that a user or group has access to (C2.2.3.14).
18. Must be able to limit the items in a drop-down box that a user or group has access to (C2.2.3.15).
19. Must allow authorized individuals to move a record from one folder and category to another (C2.2.3.16).
20. Must be able to reference or link from a record to supporting records and documents (C2.2.3.17).
21. Must provide a way for reference links to be labeled, identifying the source and target (C2.2.3.18).
22. Must be able to create and remove links between records both during and after filing of a record (C2.2.3.19).

23. Must allow authorized users the ability to define, update, and assign access permissions for reference links (C2.2.3.20).
24. Must be able to support multiple renditions of a record and be able to link to the renditions (C2.2.3.21).
25. Must be able to support versions of records and version numbering, each version with its own copy of metadata (C2.2.3.22).
26. Must be able to link record metadata to the actual record (C2.2.3.23).
27. Must allow authorized individuals the ability to modify the metadata of stored records (C2.2.3.24).
28. Must enforce data integrity, referential integrity, and relational integrity (C2.2.3.25).
29. Must be able to synchronize the data across multiple repositories (C2.2.3.26).

Filing electronic messages

1. Must be able to treat e-mail like any other record (C2.2.4.1).
2. Must be able to automatically capture the transmission and receipt of data from an e-mail record (C2.2.4.2).
3. Must provide the capability for editing e-mail fields like subject, title, author, originator and addressee(s) prior to filing (C2.2.4.2).
4. Must be able to file an e-mail as an individual record (C2.2.4.3).
5. Must be able to file attachments and portions of e-mail as separate records (C2.2.4.3).
6. Must not allow separate filings of OLE embedded objects in the e-mail body (C2.2.4.4).
7. Must not require a user to first save e-mail attachments to a hard drive prior to filing (C2.2.4.5).
8. Must provide capability to automatically link e-mail records to their attachments (C2.2.4.6).
9. Must provide authorized individuals with the capability to set up e-mail header mappings to repository properties via a user interface (C2.2.4.7).

Filing records to be later transferred or accessioned to NARA

1. Must support additional metadata properties for specific types of records (C2.2.5.1):
    a. Scanned Records:
        i. Scanned Image Format and Version (Mandatory)
        ii. Image Resolution (Mandatory)
        iii. Image Bit Depth
    b. Portable Document Format Records:
        i. Producing Application (Mandatory)
        ii. Producing Application Version (Mandatory)
        iii. PDF Version (Mandatory)
        iv. Creating Application
        v. Document Security Settings
    c. Digital Photographs:
        i. Caption (Mandatory)
        ii. Photographer
        iii. Copyright
        iv. Bit Depth
        v. Image Size
        vi. Image Source
        vii. Compression
        viii. International Color Consortium/Image Color Management (ICC/ICM) profile
        ix. Exchangeable Image File Format (EXIF) Information
    d. Web Records:
        i. File Name (mandatory)
        ii. Web Platform (mandatory)
        iii. Website Name (mandatory)
        iv. Website URL (mandatory)
        v. Capture Method (mandatory)

vi. Capture Date (mandatory)

vii. Contact (mandatory)

viii. Content Management System

Storing records

1. Must provide a single access point from the user interface to all stored records (C2.2.6.1).
2. Must prevent unauthorized access to the repository (C2.2.6.1).
3. Must be able to store any electronic file format and be able to retrieve it so that it can be viewed and edited like the original (C2.2.6.3).
4. Must allow authorized individuals the ability to move or delete records from the repository (C2.2.6.4).
5. Must raise an alert or notification if records have been removed from the repository outside of the records system (C2.2.6.5).

Screening records

1. Must be able to sort, view, save, print, search, retrieve, display, and archive folders and records (C2.2.7.1.1) based on any combination of the following:
   a. Record Category
   b. Disposition
   c. Folder and/or record metadata
2. Must be able to sort, view, save, and print lifecycle information, eligibility dates, and events of user-selected record folders and records (C2.2.7.1.2).
3. Must be able to select and order the columns of data in the search result list (C2.2.7.1.3).
4. Must be able to indicate to authorized individuals when disposition-related events have occurred (C2.2.7.1.4).
5. Must be able to sort, view, and print full and partial lists of records and folders with no assigned dispositions (C2.2.7.1.5).

Closing record folders

1. Must allow authorized individuals to close record folders to further filing (C2.2.7.2.1).
2. Must allow authorized individuals the capability to add records to a previously closed folder (C2.2.7.2.2).

Cutting off folders

1. Must allow authorized individuals to identify and present a list of folders eligible for cutoff for approval (C2.2.7.3.1).
2. Must allow authorized individuals the capability to add records to folders that have been cutoff (C2.2.7.3.2).

Freezing and unfreezing records

1. Must allow authorized individuals to freeze or suspend the retention period of folders and records (C2.2.7.4.1).
2. Must allow authorized individuals to enter a reason for why a freeze occurred (C2.2.7.4.2).
3. Must allow authorized individuals to find folders or records that are frozen (C2.2.7.4.3).
4. Must allow authorized individuals to unfreeze records and folders (C2.2.7.4.3).
5. Must allow authorized individuals to search, update, and view the reason why a record or folder is frozen (C2.2.7.4.4).

Transferring records

1. Must be able to identify folders and records that are eligible for transfer or accession (C2.2.7.5.1).
2. Must be able to export records, folders, and their metadata into an electronic format that is suitable for transfer (Media format 36 CFR 1228.270.2) (C2.2.7.5.2).
3. Must be able to export metadata for non-electronic records into an electronic format suitable for transfer (C2.2.7.5.3).
4. Must allow authorized individuals the ability to delete records and metadata that have successfully been transferred after transfer confirmation is received (C2.2.7.5.4).
5. Must allow the metadata of the transferred record to be retained (C2.2.7.5.4).
6. Must be able to provide documentation of a transfer (C2.2.7.5.5).
7. Must provide for the ability to bulk update record and folder metadata as a result of the transfer (C2.2.7.5.6).

Destroying records

1. Must allow authorized individuals to identify folders and records that are eligible for destruction (C2.2.7.6.1).
2. Must provide a second confirmation before destruction occurs (C2.2.7.6.2).
3. Must delete electronic record data so that records cannot be physically reconstructed (C2.2.7.6.3).
4. Must provide an option to select whether metadata should be retained or deleted after record destruction (C2.2.7.6.4).
5. Only authorized individuals will be allowed rights to destroy records (C2.2.7.6.5).
6. Must be able to provide documentation of destruction (C2.2.6.6.6).

Cycling vital records

1. Must allow authorized individuals the capability to specify a vital review period (C2.2.7.7.1).
2. Must be able to enter a new date after a review for the next vital record review (C2.2.7.7.2).
3. Must be able to find records that are ready to be reviewed (C2.2.7.7.3).
4. Must be able to find records by searching over the previous review date (C2.2.7.7.4).
5. Must allow an authorized individual to be able to enter a reference "as-of" date to plan for future review cycles (C2.2.7.7.5).

Searching for and retrieving records

1. Must allow authorized individuals the capability to view the File Plan (C2.2.7.8.1).
2. Must be able to search any combination of record and folder metadata (C2.2.7.8.2).
3. Must be able to search using partial matches and wildcard search over metadata (C2.2.7.8.3).
4. Must be able to search using Boolean and relational operators and be able to change the order of precedence (C2.2.7.8.4).
5. Must be able to present to the user the search result that matches the search criteria (C2.2.7.8.5).

6. Must be able to open and export the original format of the electronic data from a record to the user's machine (C2.2.7.8.6).
7. Must be able to open an e-mail record into the client e-mail application (C2.2.7.8.7).
8. Must allow authorized users a choice in saving files to their local machine or to launch directly into a viewing and editing application (C2.2.7.8.8).
9. Must be able to open earlier versions of a record with the default being the most current (C2.2.7.8.9).
10. Must be able to select any number or records and metadata from the search results (C2.2.7.8.10).
11. Must allow the user to abort a search (C2.2.7.8.11).

Access controls

1. Must provide a graphical user interface for authorized individuals to manage roles (C2.2.8.1).
2. Must ensure that the default password for the application administrator be changed from the default (C2.2.8.2).
3. Must support system authentication such as with a user ID and password, public key infrastructure (PKI), or biometrics (C2.2.8.3).
4. Must be able to provide a method for authorizing access capabilities to system users (C2.2.8.4).
5. Must be able to group users and assign privileges by group (C2.2.8.5).
6. At minimum, privileges must be available to control access to parts of the File Plan and control access to search and retrieval (C2.2.8.5).
7. If web access exists, it must provide 128-bit encryption and PKI-enabled access controls (C2.2.8.6).
8. Must support simultaneous access to the entire system by multiple users (C2.2.8.7).

System audits

1. Must provide an audit capability to log all actions, including the date, time, unique object identifiers, and user identifiers for actions taken on:
    a. User Accounts (C2.2.9.1.1)
    b. User Groups (C2.2.9.1.2)
    c. Records (C2.2.9.1.3)

   d. Associated metadata elements (C2.2.9.1.4)
   c. File Plan components (C2.2.9.1.5)

2. Must allow authorized individuals to specify exactly which items will be logged for audit (C2.2.9.2).
3. Must be able to create a report to show assigned user permissions (C2.2.9.3.1).
4. Must be able to create a report on a user's activities (C2.2.9.3.1).
5. Must be able to create a report that can facilitate the reconstruction of events around possible mishandling of records (C2.2.9.3.2).
6. Must be able to create a report that can facilitate analysis of possible system compromises (C2.2.9.3.2).
7. Must be able to create a report of denial of service history (C2.2.9.3.2).
8. Must be able to file audit reports as a record (C2.2.9.4).
9. Must allow authorized individuals to export, backup, and remove audit files from the system. (C2.2.9.5).
10. Must not allow audit logs to be edited (C2.2.9.6).

Product combinations

There are a number of mandatory requirements related to records management solutions that involve the integration of multiple products, typically the case where one product creates records and the other product is used to manage the records' disposition schedules.

These requirements do not apply to Alfresco.

System management requirements

These capabilities are frequently provided via features of the operating system or the database:

1. Must be able to automatically backup records and metadata (C2.2.11.1)
2. Must be able to store offline and at separate locations backup copies of database files, records, and metadata information (C2.2.11.2).
3. Must be able to provide recovery/backup capabilities in the event of a system failure (C2.2.11.3).
4. Must be able to rebuild from a backup copy (C2.2.11.4).

5. Must provide a way to monitor the health of the system, such as information about storage space used. Must send notifications in the event of critically low storage space (C2.2.11.5).
6. Must be able to activate a keyboard lockout feature and a screen-blanking feature (C2.2.11.6).

Additional baseline requirements

These capabilities do not necessarily apply to the Record Management system:

1. Must manage electronic calendar and task lists with record information in the system (C2.2.12.1).
2. Must treat internet e-mail or wide-area network e-mail like standard e-mail records (C2.2.12.2).
3. Must be able to maintain a method to view, copy, or print all records stored in the system. May require backwards compatibility with hardware or software or the necessity to migrate records from one format into another one (C2.2.12.3).
4. Must manage distribution lists as records (C2.2.12.4).
5. Must consult with NARA when problems arise in conforming with formats or media specifications required for accession.
6. Must schedule destruction of record copies or backups in accordance with the retention schedule (C2.2.12.6).