

# Understanding Digital Records Management

*White Paper*

**Laserfiche**

**Table of Contents**

Executive Summary.....3  
Records Management Overview .....4  
Requirements of a Records Management Application.....5  
Conclusion: Records Management in Today’s Organization.....9  
About the Author.....10

## Executive Summary

Recently, formal records management practices have become an important part of conducting business within government organizations and private industries. This is due in large part to ever stricter legislation and compliance regulations aimed at securing and archiving critical information. Most legislation and regulations have been handed down with no road map for compliance. Security and compliance officers as well as records managers have been left to fend for themselves in search of the right combination of products and procedures to ensure that complying with these regulations does not disrupt day to day operations or the ability to do business.

Fortunately, a records management standard that has evolved for several years has begun to emerge as the de facto standard across most industries. The United States Department of Defense developed a records management standard (DoD 5015.2) as a requirement for records management applications (RMAs) implemented within its departments.

Unlike other requirements though, the DoD developed very specific criteria as well as a formal testing process to determine whether a records management application meets the standard. Because of the formal testing process and the strictness of the requirements, organizations outside of the DoD have used the 5015.2 as a starting point for evaluating records management applications for their own use. Knowing that a DoD certified application has been rigorously tested against a standard that is much more demanding than the regulations they must comply with provides a great deal of comfort to compliance officers and records managers.

The goal of this paper is to describe the principles and generally accepted practices of records management. The information in this report is of a theoretical nature and not specific to any particular product or technology.

# Records Management Overview

## ***The Notion of a Record***

A record is a unit of recorded information, generated or received by an organization, which acts as evidence of activities. Most records are in the form of a document, although records in other forms are possible. The notion of a record carries with it more meaning than that of a document: a document is merely a unit of filing in a document or records management system, whereas the notion of a record encompasses the roles the underlying document plays within an organization over time, and the relationship the participant in a society have to that record, and the relationship between the record and other records.

## ***Records Management***

Records management is the application of systematic controls concerning the creation, maintenance and destruction of records required in conjunction with the operation of an organization. A chief concept underlying records management is the *life cycle concept*. This concept states that every record passes through a series of stages in which the relationship of the record towards the stewarding organization is in a distinct and classifiable mode. There are five major stages in a record's life cycle:

1. *Creation*: Information is generated and gathered into a record.
2. *Distribution and use*: The record, along with other information, is distributed among the participants in an organization in accordance with the operating practices of that organization.
3. *Storage and maintenance*: The records are filed using a logical and defined scheme into a managed repository, available for retrieval by authorized principals. The records management system is foremost here, and has responsibility for maintaining the integrity of the records, facilitating backup, and assisting users in filing and retrieval.
4. *Retention and disposition*: The information in the record has declined in value, and is removed from active accessibility. Depending on the nature of the record, it is destroyed immediately upon deactivation, or will be kept in retention for a defined period of time.
5. *Archival preservation*: Records that have a sustaining utility exceeding storage costs are preserved permanently in an archive.

The chief duties of a records management system lie at various points in this life cycle for each record. Filing, searching, retrieval, creating retention schedules, transfer, destruction, etc. all are part of managing the life cycle of a record.

## Requirements of a Records Management Application

This section describes, at a very high level, some required features for a DoD 5015.2 certified Records Management Application (RMA). Here we'll introduce and explain the jargon used in records management.

### *Record Series*

An RMA must allow for users to control the life cycle of records, to maintain the relationships among records and participants, to provide for filing according to a logical scheme, and to allow for rapid retrieval based upon partial information. RMAs are organized around the central concept of *record series*. A record series is a group of records with instructions governing the life-cycle of the constituent records. *Record folders* are created within record series as areas to file documents. Multiple Record Folders can be created beneath a single Record Series and processed at different times, but all must follow the guidelines dictated by their Record Series. That is, record folders are organized hierarchically under series.

Each record corresponds to at least one document in a record folder. A document is filed in exactly one record folder. The RMA must allow records to be re-filed into different folders or series after the initial filing. Every object has a unique identifier during the lifetime of the RMA.

### *Metadata*

Each record, record series and folder maintains a set of *metadata fields*. Every metadata field has a human readable name or designator, and corresponding data that can be stored in the field. Some fields are *mandatory* and every object must be assigned valid data into these fields when filing, while other fields can be filled in optionally. The RMA should automatically fill and maintain fields as is reasonable and appropriate, although it must also provide for specifically user-created fields. There must be facilities to search for objects by field contents. The RMA must have a way to constrain the type of data that can be entered for a field. The RMA must limit the general editing of all metadata to the time of filing, except for authorized users who will have the ability to edit and correct filing errors. It should be noted that if a user does not have rights to edit a mandatory template field that is not auto-populated, they will not be able to file records using that template.

### *Linking*

The RMA must allow the users to define and establish relationships between documents, in the form of *document links*. Each link type has a unique human readable name, and each link contains the identifier of the source and linked to documents. There must be a way to view which documents are linked to, linked from, and by which link type for each document. There may also be a need to define (or allow for the defining) of events based on these links. Some examples of document links are superceded/successor records, multiple renditions, email/attachments, supporting documents and incremented versioning. As a form of metadata, document links can be established by all users at the time of filing and created/modified/removed post-filing by authorized users only.

### ***Versioning***

The RMA must allow the users to establish record versioning, which is a special case of document relationships. Versioning is used to indicate an auto-incremented sequence of revisions to a particular record. Versions must all be retrievable as if they were independent documents and contain their own metadata, although the metadata for new versions can be based on that of a prior version. Versions can also be spread among multiple record series and have independent dispositions. The RMA must clearly indicate if a record is involved in versioning and if it is the most recent version.

### ***Security Markings***

The RMA must allow the RM to define *Security Markings*, and to allow users to assign markings to records upon filing. These markings serve as a security based metadata field and are intended to define and restrict access as well as aiding in classification and retrieval. The RMA may also allow the RM to define *informational markings* at the time of filing. These markings are non-security metadata, and are intended solely as an aid to classification and retrieval. The presence of this second form of markings is not mandated by the RMA requirements. Regardless of being security-based, only authorized users only can modify/remove Supplemental Markings post-filing.

### ***Vital Records***

The RMA must maintain which records are deemed *vital*, essential agency records that are subject to periodic review and update. Examples of vital records might be either emergency operating records or legal and financial rights records. There must be a way to assign a review cycle to vital records and set when they were last reviewed. There must also be ways to retrieve all vital records, determine when they were last reviewed or obtain a list of all the records due for review at a certain time.

Vital Record status is determined by the Record Folder, such that all records inside a Vital Records Folder are considered Vital Records. Vital Records Cycle periods may be any time range from daily on up, and may also be specified by the RM. The Vital Record review date and cycle period can be set by authorized users only.

### ***Cutoff***

Each record series has an associated set of retention and disposition instructions. This must consist of all of the following: *cutoff criteria*, which determines when the records in a series can be cutoff; a *retention period*, which is given as one or more intervals of time in between cutoff and each action; a list of *disposition actions*, which describes the actions that will happen to an inactive record after each retention period is over.

All record series will have a non-zero value for cutoff criteria, although the possible numbers of retention and disposition events could range from 0 to infinite. A retention period that occurs between cutoff and the first disposition action can

also be known as the *hold period*. Logically, disposition instructions can be segregated into cutoff criteria, and what happens after cutoff.

Cutoff criteria can take three forms: *time disposition*, *event disposition*, and *time-event disposition*. The cutoff criteria define the *cutoff eligibility* for record folders located within a given record series. In time dispositions, the record series defines a time-based cycle period and the records in that series become eligible for cutoff once the period has finished (A monthly cutoff period would make records eligible for cutoff at the first day of the following month).

In event disposition, eligibility occurs when an external event has occurred. The specific trigger for the event is defined on the individual folder level within the record series. The RM will generally have to indicate to the RMA that the event has occurred, although there are circumstances where it would be preferable for the RMA to automatically note an occurred event (For example, when the event involves changes recorded within the RMA itself).

In time-event disposition, the triggering of the event inactivates the record, although it is not eligible for cutoff until further time-based criteria is passed. An example of this would be a record folder whose contents would be eligible for cutoff on the first day following the month containing the relevant event.

### ***Closing Records***

When the RM or RMA indicates that an event has occurred for a record folder with an Event or Time-Event record series, the folder is *closed* (no new records can be filed) and all the records in the folder are held *inactive* (no modifications allowed). For Time record series, these cannot happen until after the folder is cutoff. Anytime after a record folder is eligible for cutoff, the RM may elect to cutoff the folder. Since a record series acts to define the retention/disposition process, it can never be cutoff itself – all cutoff and further disposition events must occur at the folder or record level. While the RMA maintains the status of cutoff eligibility, it is the RM that must initiate cutoff - there is no automatic cutoff of folders by the RMA. Cutting off a folder prompts the beginning of the retention period and also closes and inactivates folders located within Time series. During the interval between any folder being closed and being cutoff (regardless of cutoff eligibility), the RM can *reopen* the folder allowing for further filing and re-activation of records. For Event and Time-Event series, this implies that the event did not occur, clearing the original event date and removing any cutoff eligibility the folder may have had.

### ***Retention***

The first retention period, known as the hold period, can be any duration including zero. Once the retention period is over, the records in a folder are said to become *eligible for disposition* and may then *enter disposition* by having a further disposition action performed upon them. During the hold period, the records are stored within the current file area and must still be accessible within the system. Anytime during the hold period, the RM may choose to *un-cutoff* folders within an event or time-event series. This would be done primarily to invalidate inappropriate event eligibility and has the same effects of reopening a non-cutoff folder. Since it does not make sense to invalidate a purely time eligibility, you cannot un-cutoff folders contained within time series. When a folder is un-cutoff,

the RMA changes the status of the event to a non-occurred status. Regardless of disposition eligibility status, the hold period does not end until a further disposition action is performed on the specific record folder, moving it out of the current file area.

### ***Disposition***

After the hold period is over, inactive documents can be subject to one or more disposition actions. There are two types of available disposition actions that must be handled by the RMA, *interim transfers* and *final disposition*. Zero or more interim transfers can be selected. If selected, these actions will be applied in sequence and there will be a retention period between each transfer. The available actions for final disposition are *accession*, and *destruction* they always occur after any and all transfers have taken place. At most one final disposition can be chosen.

Interim transfers and final dispositions also differ in their eligibility requirements. The eligibility requirement for a final disposition is a strict rule – a final disposition cannot be performed if the record folder is not specifically eligible for it. Interim transfers are much more lenient, however, allowing for transfers to take place when they are not necessarily eligible, in different orders than outlined by the record series, or even to be outright skipped. This is because the record is still under the authority of the original institution and they can choose how to handle it.

Transfer is the act of moving records out of the current storage area. For physical records, this might entail moving boxes of records out of prime office-space into low-cost warehouses. For electronic records, this might mean exporting the documents to optical media and then deleting the online copies. Destruction is the act of permanently destroying documents. For most RMAs, this is deletion. Records located within Record Series designated as containing *Permanent Records* cannot be destroyed. *Accession* is very similar to transfer, with the prime difference that transfer involves movement of records while still maintaining authority over the records, whereas accession is the transfer of responsibility and authority over the records to another organization, generally for archival purposes. Records with no final disposition are held inactive but available for access in perpetuity.

The RMA must allow for the exporting of entire record folders and their metadata values for transfer and accession events. Following confirmation of a successful transfer, the RMA will be instructed to maintain the records, maintain just the metadata or completely delete the records. Accession or Destruction events require the RMA to delete the electronic records, although the RM must be allowed to specify whether to save and store the associated metadata components. Following each transfer, the next action may be another transfer, or it may be a final disposition. No action is taken upon the record after final disposition.

### ***Freezing***

At anytime, a folder may be *frozen* by the RM. The RMA must also request a freeze reason from the RM upon freezing. The act of freezing a folder halts all dispositions on it. Furthermore, when a folder is frozen, no records may be removed from the folder (regardless of whether they were in the folder when the freeze event occurred), and no records in the frozen folder may be modified. If the folder is active, then the folder may not be cutoff, even if the folder would

normally be eligible for cutoff. If the folder is being held inactive, it will not enter disposition, even after the retention period is over. If the folder is held in disposition, it will not progress to the next action. A frozen folder may be *unfrozen* by the RM once it can re-enter normal retention/disposition.

## **Conclusion: Records Management in Today's Organization**

Once a file plan has been established in an organization, an RMA will manage the document lifecycle as defined within each record series. Users simply file records in the appropriate folder, and they will be prompted to enter any required metadata that hasn't been automatically captured and the RMA will take over. Records managers can run reports detailing where records are in their lifecycle, which records should be reviewed and which records are eligible for transfer, accession or destruction. Additionally, all system activity is logged, providing an audit trail that tracks the entire lifecycle of the records that can be used to prove adherence to the records management plan and adherence to legislation and/or compliance regulations.

While their records management requirements might not be as detailed as the DoD standard, organizations can use all or some of the tools provided to implement a solution that fits their exact needs. The right RMA will provide all the tools necessary to design and implement a DoD compliant file plan for the management of all imaged, electronic and physical records

## **About the Author**

Laserfiche, a division of Compulink Management Center, Inc.

Since 1987, Laserfiche has provided document imaging and management solutions for over 21,000 government and business entities. Laserfiche Records Management Edition was developed using the DoD 5015.2 standard as a component of the design specifications. The software was tested by the Joint Interoperability Test Command and certified as compliant in September 2003.

Laserfiche

A division of Compulink Management Center, Inc.

3545 Long Beach Blvd.  
Long Beach, CA 90807 USA  
+1 562.988.1688  
[www.laserfiche.com](http://www.laserfiche.com)

© 2005 Compulink Management Center, Inc. All rights reserved. Laserfiche is a registered trademark of Compulink Management Center, Inc. Product and service names referenced herein may be trademarks of Compulink Management Center, Inc. All other trademarks are properties of their respective companies. Due to continuing product development, product specifications and capabilities are subject to change without notice. Printed in the USA.

The information contained in this document represents the current view of Compulink Management Center, Inc. on the issues discussed as of the date of publication. Because Compulink must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Compulink, and Compulink cannot guarantee the accuracy of any information presented after the date of publication. This paper is for informational purposes only. Compulink makes no warranties, express or implied, as to the information in this document.