

# EMC Documentum RM v6.0 by EMC Corporation

---

## EMC Documentum RM Summary Report

The Joint Interoperability Test Command (JITC) tested EMC Corporation's EMC Documentum Records Manager (RM) Version (v) 6.0, a web-based document and Records Management Application (RMA), at the EMC facility in Ottawa, Canada, from 23 October through 01 November 2007.

The JITC verified that EMC Documentum RM v6.0 is compliant with Chapter 2, Mandatory Requirements, and Chapter 4, Management of Classified Records, of Department of Defense 5015.2 Standard, "Design Criteria Standard for Electronic Records Management Software Applications," dated 19 June 2002. The JITC verified compliance using v7.5 of the RMA Compliance Test Procedures.

### TABLE OF CONTENTS

- [Section 1. Product Identification](#)
  - [Section 2. Test Configuration](#)
  - [Section 3. RMA Mandatory Requirements](#)
  - [Section 4. Non-Mandatory Features Demonstrated](#)
  - [Section 5. Management of Classified Records](#)
- 

## 1. Product Identification

EMC Documentum RM v6.0, hereafter referred to as Documentum RM, is a web-based document and records management application.

## 2. Test Configuration

The testbed hardware configuration consisted of:

- One server running Microsoft (MS) Windows Server 2003 (SP2). Installed software included Apache Tomcat v5.5 and Brava! Server v5.3 (SP3).
- One server running Microsoft (MS) Windows Server 2003 (SP2). Installed software included Apache Tomcat v5.5 configured for Secure Sockets Layer (SSL).
- One server running Microsoft (MS) Windows Server 2003 (SP2). Installed software included EMC Documentum Content Server v6.0 and MS SQL Server 2005 (SP1).
- One server running Microsoft (MS) Windows Server 2003 (SP2). Installed software included BEA v9.2.
- One server running Microsoft (MS) Windows Server 2003 (SP2). Installed software included EMC Documentum Content Server v6.0 and Oracle 10g (v10.2.0.1).
- One workstation running MS Windows 2002 XP Professional (SP2). Installed software included MS Internet Explorer v6.0 (SP1), MS Office Professional 2003 (SP2), and MS Outlook 2003 (SP2).
- One workstation running MS Windows Vista Premium. Installed software included Firefox v2.0.0.3 and MS Office Professional 2003 (SP2).

In a subsequent configuration, the JITC repeated the compliance test using EMC Centera SDK 3.0 (SP1) as the record repository.

### **3. RMA Mandatory Requirements**

#### **3.1 *Managing Records [C2.1.1.]***

Documentum RM manages electronic, non-electronic, and e-mail records. It stores electronic records either on the NTFS or in the EMC Centera repository, and maintains them in their original, native file format. Users maintain records stored on other media, such as paper, diskette, or tape by adding metadata through the user interface.

#### **3.2 *Accommodating Dates and Date Logic [C2.1.2.]***

Documentum RM uses a 4-digit year format to store and display dates and recognizes leap years including the year 2000. The product accepts user input of valid dates from current, previous, and future centuries.

#### **3.3 *Implementing Standard Data [C2.1.3.]***

Documentum RM provides the capability to implement standard data elements. It can be configured with all the data elements as defined in DoD 5015.2-STD. Records managers can configure Documentum RM with additional fields for custom use and can assign pick lists and default values to assist users in filing records.

#### **3.4 *Backward Compatibility [C2.1.4.]***

Documentum RM demonstrated backward compatibility by loading Documentum RM v6.0 with the backup of the Documentum RM v5.3 database that was tested compliant to Chapter 2 and Chapter 4 in August 2006.

#### **3.5 *Accessibility [C2.1.5.]***

EMC Corporation provided the 508 Voluntary Product Accessibility Templates (VPATs). They are included in Appendix B of the detailed test report.

#### **3.6 *Implementing File Plans [C2.2.1.]***

Documentum RM provides the required capabilities for creating and maintaining disposition schedules (known as retention policies) and file plans.

Records managers create disposition schedules and assign them to record categories or folders. If a disposition schedule is assigned at the record category level, folders under that level inherit the same disposition schedule, unless a different disposition schedule is specified at that level.

#### **3.7 *Scheduling Records [C2.2.2.]***

Documentum RM tracks the disposition schedules for screening and disposition processing. Records managers reschedule files by assigning a different disposition schedule to the record category/folder or by altering the disposal schedule. This process will assign the new disposition schedule to the record category/folder for all future declared records; current records would retain the previous disposition schedule. To reassign the current records with the new disposition schedule, record manager would

disqualify the associated record category/folder then requalify it, which would reschedule all record categories/folders associated with that schedule.

### **3.8 Declaring and Filing Records [C2.2.3.]**

Documentum RM provides the capability to file electronic and non-electronic records. Users file records by logging into their workspace, selecting a document, and "Records" and "Declare as Formal Record." Documentum RM presents a record profile. Users assign a record category/folder, complete the metadata, and click "OK."

At the time of filing, Documentum RM assigns a unique record identifier and a date/time stamp to each record. The date/time stamp serves as the required "Date Filed" profile field. Users cannot modify either field.

### **3.9 Filing E-mail Messages [C2.2.4.]**

Documentum RM provides the capability to file e-mail messages from MS Outlook. Documentum RM automatically captures message transmission and receipt data to populate the "Author/Originator," "Addressee(s)," "Other Addressee(s)," "Publication Date," and "Subject" record profile fields.

When filing an MS Outlook e-mail with attachment(s), Documentum RM presents users with two options:

- **One Record.** Encapsulates the .msg file into a proprietary EMC Mail Format and stores it in the repository. (Documentum RM converts the message back to an .msg format when the record is transferred or exported.) Users can save attachments to their hard drives and file them as any other electronic document.
- **Individual Records.** Encapsulates the .msg file into a proprietary EMC Mail Format and stores it in the repository. In addition, it stores each attachment separately in its native file format.

### **3.10 Storing Records [C2.2.5.]**

Documentum RM uses the server's file system for storing and preserving electronic records. As an alternative, organizations can store records on EMC Centera SDK 3.0 (SP1). The permissions assigned at the series, folder, and document levels determine who has access to the records and what each user can do with those records. Only users with appropriate access can delete records.

File plan and document profile data are stored separately from the actual records in a relational database. MS SQL Server 2005 (SP1) and Oracle 10g provided the database during the compliance test.

### **3.11 Screening Records [C2.2.6.1.]**

Documentum RM provides record screening functionality via the Qualification Manager. Records managers can enter future dates to facilitate planning.

To promote items to the next step in their lifecycle, records managers use the Promotion Manager. This also allows the use of future dates; however, records managers can only promote those items that are currently due for promotion.

### **3.12 Closing Record Folders [C2.2.6.2.]**

Documentum RM offers authorized users the ability to close folders. To close a folder to further filing, authorized users select "Records" and "Close Folder." Users cannot file records into closed folders. When necessary, records managers can re-open folders to further filing.

### **3.13 Cutting Off Record Folders [C2.2.6.3.]**

Documentum RM provides the capability to cutoff record folders.

### **3.14 Freezing/Unfreezing Records [C2.2.6.4.]**

Documentum RM provides the capability to freeze and unfreeze categories and folders by creating and applying a "Retention Markup" to the record category/folder. If a record category/folder is frozen, records managers cannot execute disposition actions on that item.

### **3.15 Transferring Records [C2.2.6.5.]**

Records managers access the Disposition Manager when they are ready to transfer record folders. They run a search to find all records/folders/categories that qualify for transfer. They select the items and click "Dispose" to perform the transfer.

### **3.16 Destroying Records [C2.2.6.6.]**

Records managers access the Disposition Manager when they are ready to destroy record folders. From the Disposition Manager, they run a search to find all record folders that qualify for destruction. They select the items and click "Dispose" to perform the destruction. Deleted records are not recoverable with a file recovery utility.

### **3.17 Cycling Vital Records [C2.2.6.7.]**

Documentum RM provides the capability cycle vital records. Records managers create "Retention Markups" pertaining to the vital records cycle and assign these to selected record categories/folders. When those categories/folders are due for review, Documentum RM alerts the designated reviewer, either via e-mail or by sending a reminder to the reviewer's inbox.

### **3.18 Searching for and Retrieving Records [C2.2.6.8.]**

From the main screen, Documentum RM offers users the ability to perform quick searches. Users enter a search term and click "Go." For more complex searches, Documentum RM offers an advanced search. Users build complex queries using any combination of metadata fields.

Users can select which fields to display in the search results list and specify the order. They also have the option to save commonly used searches. Records are retrieved based on the user's permissions. Authorized users can export copies of records to the workstation.

### **3.19 Access Controls [C2.2.7.]**

Documentum RM provides several methods to control user access to records held in the repository. This control is managed in several ways: user/group/role level access, file plan access, and supplemental markings. Combinations of these functions ensure that records can be held securely and can only be accessed by users with the permission to view or modify those records.

### **3.20 System Audits [C2.2.8.]**

Documentum RM offers the capability to perform audit logging. The system audit log captures all activity that occurs in the repository to include delete, edit, create, retrieve, browse, and search.

Documentum RM collects the audit metadata specified in the Standard.

### **3.21 System Management Requirements [C2.2.9.]**

The operating system (MS Windows Server 2003 (SP2)) and the database management system (MS SQL Server 2005 (SP1)) or Oracle 10g v10.2.0.1 provide the required system management capabilities.

## **4. Non-Mandatory Features Demonstrated**

### **4.1 Retrieval Assistance Capability [C3.2.7.]**

Documentum RM includes an advanced search capability accessible to all users through the advanced search template. Users can perform a search on any metadata field and use Boolean operators to narrow the search results list. Users can save their search criteria for frequent use.

### **4.2 Web Capability [C3.2.15.]**

Documentum RM is a fully web-based RMA. All records (physical and electronic) and records management functions are URL accessible. The application is available through Internet Explorer 6.0 (SP1) or Firefox v2.0.0.3.

## **5 Management of Classified Records**

Documentum RM was configured to satisfy all Chapter 4 requirements. The following paragraphs highlight Documentum RM's implementation of specific Chapter 4 requirements.

### **5.1 Managing Classified Records [C4.1.]**

Documentum RM provides the capability to manage classified records. Documentum RM can be configured such that users have the option of filing classified and unclassified records on a single installation.

### **5.2 Mandatory Metadata [C4.1.1.]**

Documentum RM comes with all the metadata elements for classified records as specified in Table C4.T1. of the Standard. When filing classified records, users select a security classification (one of Confidential, Secret, or Top Secret). When a user selects a classification, Documentum RM prompts the user to populate the security-related fields before saving the record.

### **5.3 Classification Guides [C4.1.10.]**

Documentum RM supports classification guides. Users click on the classification guide link to display the available classification guide indicators. They select the classification guide indicator they want to use and then select a topic. Documentum RM copies the information from the guide entry into the relevant fields of the classified metadata template.

#### **5.4 *Editing Records [C4.1.12.]***

Authorized users can search for classified records due for downgrade or declassification. If the classification status of a record changes, (i.e., the record's classification is upgraded, downgraded, or declassified), authorized users are allowed to edit the classified record metadata to reflect the change.

#### **5.5 *Restricted Data and Formerly Restricted Data [C4.1.13.]***

Documentum RM provides the capability to handle classified records with the "Restricted Data" and "Formerly Restricted Data" supplemental markings.

#### **5.6 *Record History Audit [C4.1.16.]***

Documentum RM's record history audit captures replaced metadata values, and the user who entered that value. Users can view, copy, save, and print the audit log based on their access permissions. The capability to delete the audit log is reserved for system administrators only.

#### **5.7 *Access Control [C4.1.20.]***

Documentum RM provides the capability to restrict access to records and their metadata based on access criteria. Users are assigned a classification (security) level of "Top Secret," "Secret," "Confidential," or "No Markings." Security levels are hierarchical, therefore, users assigned a "Secret" security level will only see records marked "Secret" and below.

Users are also assigned supplemental markings. Supplemental markings do not override a user's access, but work in conjunction with the user's designated classification level to partition access.

---

Last revision: **15 November 2007**