IBM DB2 Records Manager v4.1
by IBM Corporation

IBM DB2 Records Manager v4.1 Summary Report

The Joint Interoperability Test Command (JITC) tested IBM Corporation's IBM DB2 Records Manager Version (v) 4.1, a web-based records management application (RMA), at the IBM facility in Ottawa, Canada from July 26 through 30, 2004.

JITC verified IBM DB2 Records Manager v4.1 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. JITC verified compliance using 7.5 of "RMA Compliance Test Procedures."

TABLE OF CONTENTS

1. Product Identification

IBM DB2 Records Manager v4.1 (IRM) is a web-based records management system designed for integration into document management and workflow environments. It can also be used as a stand-alone application.

2. Test Configuration

The test configuration consisted of:

- One engine server running Microsoft (MS) Windows 2000 Server (SP4). Installed software included Websphere Application Server v5.1, IBM HTTP Server 1.3.28, Microsoft Office 2000 (SR1), MS Outlook 2000 (SR1), MS Internet Explorer 6.0 (SP1), and IBM DB2 v8.1 FP5 (client).
- One database server running Microsoft (MS) Windows 2000 Server (SP4). Installed software included IBM DB2 v8.1 FP5 (server).
- One exchange server running Microsoft (MS) Windows 2000 Server (SP4). Installed software included Microsoft Exchange 5.5 (SP3) and MS Internet Explorer 6.0 (SP1).

3. RMA Mandatory Requirements

3.1 Managing Records [C2.1.1.]

IRM manages electronic and non-electronic documents. It stores electronic documents in its repository and maintains them in their original, native file format. Users maintain documents stored on other media, such as paper, diskette, or tape, as records by adding profile data through the user interface.

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

IRM stores and displays dates using a 4-digit year format, and recognize leap years including the year 2000. IRM accepts user input of valid dates from current, previous and future centuries.

3.3 Implementing Standard Data [C2.1.3.]

IRM provides the capability to implement standardized data. Records managers create data entry templates. They can assign default values to the metadata fields and can also assign default templates to groups and/or users. In addition, they can create pick lists to assist the user in filling out the templates.

3.4 Backwards Compatibility [C2.1.4.]

JITC verified backwards compatibility by upgrading from IBM DB2 Records Manager v3.1 to IBM DB2 Records Manager v4.1.

3.5 Accessibility [C2.1.5.]

IBM Corporation provided the 508 Voluntary Product Accessibility Templates (VPATS) provided as appendices to the detailed test report.

3.6 Implementing File Plan [C2.2.1.]

IRM provides the required capabilities for creating and maintaining a file plan through the File Plan Administration screen. File plan information is stored in a relational database and consists of record series, record categories, record folders, and documents.

Disposition instructions are encompassed in the Life Cycle Code. Life cycle codes are then assigned to the record plan components. If a life cycle code is assigned at the series level, components under that series inherit that code unless another life cycle code is specified for that component.

Access to the associated IRM functions is granted/restricted through the assignment of privileges to groups and/or users. IBM provides support for multiple levels of file plan access. During the test “privileged” users were able to create and manage record folders.

3.7 Scheduling Records [C2.2.2.]

IRM provides the capability to schedule records and automatically tracks the disposition schedules for screening and disposition processing. Record lifecycles are implemented using phases through which each record must pass for the period of time designated in the associate lifecycle codes.

3.8 Declaring and Filing Records [C2.2.3.]

Users can file directly into the IRM repository from the web browser by navigating to the appropriate record category/folder and clicking the “Actions” link. They select “Add: Document.” IRM presents the record profile. Users complete the profile and select "Save." If they are adding a non-electronic record, the IRM files the record. If they are filing an electronic record, IRM prompts the user to add the electronic file to the repository and then files the record.

At the time of filing, IRM 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 Records [C2.2.4.]

IRM provides the capability to file messages from MS Outlook 2000. It automatically captures message transmission and receipt data to populate the Author/Originator, Addressee(s), Document Creation Date, and Subject record profile fields.

When filing Outlook e-mail that has an attachment(s), IRM presents the user with three filing options.

- **Single Record**. Stores the e-mail as an .msg file (which includes the attachments).
- **E-mail and Each Attachment as a Record**. Stores the e-mail (without attachments) as an .msg file (which includes the attachments) and, in addition, stores each attachment separately in its native file format.
- **Both**. Files the e-mail as a single record and also files the e-mail and each attachment as a record.

3.10 Storing Records [C2.2.5.]

IRM uses the server's NT File System (NTFS) for storing and preserving electronic records. The permissions granted at the series, category, folder, and document level determine who has access to the records and what they can do with those records. Only users with appropriate access can delete records from the repository.

File plan and document profile data are stored separately from the actual records in a relational database. IBM DB2 v8.1 FP5 provided the database during the certification test.

3.11 Screening Records [C2.2.6.1.]

Records managers perform screening functions through the Life Cycle Operations screens. From here, they design queries and reports for information relating to the records' life cycle, such as finding folders due for cutoff, transfer, or destruction. IBM added a user-defined "Event Description" field to assist records managers in finding event-related folders.

Version 4.1 treats screening and disposition queries as batch jobs that can be scheduled to run at the Record Manager's convenience. The jobs can also run immediately and show the status on the status screen.

3.12 Closing Record Folders [C2.2.6.2.]

IRM offers records managers and privileged users the ability to close folders through the folder profile-editing screen.

3.13 Cutting Off Record Folders [C2.2.6.3.]

To cut off records, records managers search for all folders eligible for cutoff on a certain date (called the Reference Date). IRM gives the records manager an opportunity to verify the life cycle transition. If the records manager verifies the change, IRM applies the Life Cycle Date to the folder. By cutting off the folder, all records within that folder are cutoff as well. IRM creates two XML transition log files consisting of the metadata transfer file and the Life Cycle Operation Log file.

Records managers can also choose to perform cutoff at the category or series level, in which case all folders and documents under that category or series are cutoff.

3.14 Freezing/Unfreezing Records [C2.2.6.4.]

IRM provides the ability to freeze and unfreeze records at all levels of the file plan. If a record series is frozen, all categories, folders, and documents in that series do not qualify for disposition processing. If a record in a folder is frozen, the folder will not qualify for disposition processing.

3.15 Transferring Records [C2.2.6.5.]

IRM distinguishes between record transfers and record accessions. Transfers are treated as interim transfers, where a record is sent to secondary storage but the organization retains responsibility for that record. In this case, the actual file is removed from the repository, but the record metadata is kept within IRM. When IRM accessions records, it surrenders ownership of the record to another authority and the files and metadata are removed from the repository.

Interim transfers are set up to execute before a record enters the specified phase of the lifecycle. IRM transfers the records out, but continues to track the lifecycle through accession or destruction.

To search for folders due for accession, the records manager queries the RMA. IRM presents a list of those folders and the records manager verifies they should be accessioned. IRM then writes the affected electronic files, a transmission log, and the folders and record metadata to a user specified directory. IRM deletes these items from the repository and database. The transmission log and metadata are in XML format.

3.16 Destroying Records [C2.2.6.6.]

To destroy records, the records manager searches on those folders due for destruction, selects them, and verifies that the folders should be destroyed. IRM then deletes the folders (and any records within those folders) from the repository and database.

Records cannot be reconstructed once they have been deleted.

3.17 Cycle Vital Records [C2.2.6.7.]

IRM provides the ability to gather records based on cycling dates and to do bulk updates of cycle dates after records have been reviewed. During the test, IBM attached logic to the vital record review date fields that sent email to a specified records manager when the folders were due for vital records review.

3.18 Searching and Retrieving Records [C2.2.6.8.]

IRM provides the required capability to search for and retrieve records. Inter-field operators are available in the event the user wants to perform nested searches. Users also have an opportunity to select exactly what fields should be presented in the search results. IRM allows users to download copies of the record to their hard drives.

IRM shows all versions and renditions available for retrieval and displays a message that a newer version is available. Users can access previous versions through the renditions screen.

3.19 Access Control [C2.2.7.]

Records managers assign IRM functional access to series, categories, folders, and records at the user and/or group level. IRM supports multiple-user access. During most of the certification test, two users worked simultaneously performing various functions including filing system maintenance, document filing, record retrieval, reporting, and disposition activities.

3.20 System Audits [C2.2.8.]

Administrators determine what events to log for each IRM object type. Examples of audited events include add, delete, life cycle transitions, copy, update, view, and move. IRM can also audit user events such as log on, log off, failed log on, and each time a user initiates a life cycle management operation.

IBM collects the audit metadata specified in the Standard, however, it does not collect sufficient data to adequately reconstruct a user's attempts at unauthorized access.

3.21 System Management Requirements [C2.2.9.]

MS Windows 2000 Advanced Server and IBM DB2 v8.1 FP5 provide the required system management capabilities.

4. Non-Mandatory Features Demonstrated

4.1 Global Changes [C3.2.1.]

IRM provides the ability to make global changes to IRM objects. Global changes are an extension of reporting. Once users generate reports, they can perform a mass update on the report results by selecting the desired files and Bulk Operation. IRM presents a template with all fields available to the object through which users perform the global change.

4.2 On-line Help [C3.2.5.]

IRM provides on-line documentation. Users access on-line help via a Help hyperlink from the main form and can access the contents, index, or search on the topic of their choice. Help was also available on every page of IRM.

4.4 File Plan Component Selection/Search Capability [C3.2.10.]

IRM allows users to browse the file plan through the file plan administration tab and supports searches on specific file components through the search screen.

4.5 Web Capability [C3.2.15.]

IRM is a web-based solution. The application is available through MS Internet Explorer 6 (SP1) and IBM HTTP Server 1.3.28 to serve the pages.

5 Management of Classified Records

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

5.1 Managing Classified Records [C4.1.]

IRM provides the capability to manage classified records. When filing classified records, uses complete the "Security Classification Info" section of the filing template.

5.2 Mandatory Metadata [C4.1.1.]

IRM is configured to provide all the classified metadata elements as specified in Table C4.T1 of the DOD 5015.2-STD.

5.3 Classification Guides [C4.1.10.]

IRM implements classification guides as tables. 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. IRM 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 the record changes, authorized users are allowed to edit the classified record metadata.

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

IRM provides the capability to handle classified records with the "Restricted Data" and "Formerly Restricted Data" supplemental markings. When users select either marking, IRM blanks out the "Downgrade On" and "Declassify On" fields.

5.6 Record History Audit [C4.1.16.]

IRM'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.

5.7 Access Control [C4.1.20.]

IRM 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 Unclassified. Security levels are hierarchical, therefore, those users assigned a "Secret" security level will only see documents 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. Additionally, IRM has the ability to restrict access on user-defined fields.

Last revision: ***18 August 2004***