IBM DB2 Records Manager

Version 4.1.3

Designing a DoD 5015.2 Compliant Solution

DB2 IBM DB2 Records Manager

Version 4.1.3

Designing a DoD 5015.2 Compliant Solution

Notices:

Before using this information and the product it supports, read the information in ″Notices″ in the back of this book.

First Edition (November 2006)

This edition applies to Version 4.1.3 of IBM DB2 Records Manager (product number 5724-E68) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

---

[1] The DoD enabled database is meant to provide you with a 'head start' to configuring your data for certification. While it was correct at the time of its creation, DoD testing procedures and data evolve over time. It is not meant as the final and complete set of data. IBM makes no warranties expressly or implied regarding the completeness or correctness of the data during your testing.

Chapter 1. About this book

This document describes how to use DB2 Records Manager to provide United States Department of Defense 5015.2 compliant solutions. It also provides a detailed architectural overview of DB2 Records Manager to assist partners in designing their own integrated solutions.

This guide includes the following:

- A description of the concepts and architectural overview explaining what is required, and a possible integration strategy to meet those requirements
- Explanations for the DoD test cases, and how to use Records Manager to pass these test cases
- A tabular Summary listing all of the DoD 5015.2 requirements with their corresponding Host requirements, including details about the steps a Host application must take to meet these requirements

Who should use this guide

Use this guide if you require information about providing DoD compliant solutions, or for designing your own solutions.

How to use this guide

This guide uses the following conventions:

bold	Identifies commands, flags, keywords, files, directories, and other items whose names are predefined by the system.
italics	Identifies parameters with actual names or values that you must supply.
`monospace`	Identifies examples of specific data values, examples, of text similar to what you might see displayed, examples of portions of program code similar to what you might write, messages from the system, or information you should actually type.

Ensure that you examine the IBM DB2 Records Manager readme file for additional information. You can find this readme file in the location *install-directory/readme.txt*, where *install-directory* is the directory where you installed IBM DB2 Records Manager.

Product Publications

You can view the following documentation from the IBM® DB2® Records Manager Web site at *http://www-3.ibm.com/software/data/cm/cmgr/rm/*:

Document	Part Number
IBM DB2 Records Manager Planning and Installing Guide	SC18-9185-01
IBM DB2 Records Manager Technical Reference	SC18-9181-01
IBM DB2 Records Administrator's Guide	SC18-9180-01

Document	Part Number
IBM DB2 Records Manager Import Export Guide	SC18-9183-01
IBM DB2 Records Manager Tutorial Guide	SC18-9886-00

Related Publications

The DB2 Universal Database™ publication Web site contains information related to IBM DB2 Records Manager. The DB2 Web site is located at:

http://www.ibm.com/software/data/db2/library/

Sending your comments

Your feedback helps IBM to provide quality information. Send any comments that you have about this book, or about other Records Manager documentation. You can use either of the following methods to provide comments:

- Send you comments from the Web. Visit the online Readers' Comment Form (RCF) for IBM Data Management page at:

  http://www.ibm.com/software/data/rcf
- Send your comments by e-mail to **comments@vnet.ibm.com**. Ensure that you include the name and part number of the book, if applicable. If you are commenting on specific text, include the location of the text within the documentation set (for example, a chapter and section title, a table number, a page number, or a help topic title).

Contacting IBM software support

The IBM software support Internet site provides you with self-help resources and electronic problem submission. The IBM software support home page can be found at *www.ibm.com/software/support*. The IBM DB2 Records Manager support site can be found at *http://www.ibm.com/software/data/cm/cmgr/rm*.

Voice support is available to all current contract holders via a telephone number in your country (where available). For specific country phone numbers, see to the IBM Software Support Handbook, Appendix B: Contact Information, found at *http://techsupport.services.ibm.com/guides/webhndbk.pdf*.

Chapter 2. Introduction

IBM DB2 Records Manager enables content or document management applications to provide sophisticated records management capabilities. By integrating with the Records Manager Engine, applications can take advantage of pre-defined libraries for File Plan Design and Administration, Record's Life Cycle Administration and Retention Management, and advanced Reporting capabilities. An application that uses these capabilities can be classified as electronically records-enabled.

Applications that want their electronic records-enabled solutions to be certified as DoD 5015.2 compliant can use the development model outlined in this guide. A DoD 5015.2 certified product must meet all of the MANDATORY REQUIREMENTS as outlined in chapter 2 of the DoD 5015.2-STD RMA DESIGN CRITERIA STANDARD. In addition, to be certified as supporting management of classified records, they must also meet the requirements in chapter 4 of the standard. The resulting product can be certified compliant with the DoD 5015.2 standard, and placed on the compliant application roster.

This guide provides information on the tools, resources and techniques used to develop a DoD 5015.2 compliant solution. The IBM DB2 Records Manager Toolkit includes a number of prepared resources, including a DoD database image, and logic and email extensions.

For information about the DoD 5015.2-STD RMA DESIGN CRITERIA STANDARD, see the Joint Interoperability Test Command Records Management Application (RMA) Testing Program at *http://jitc.fhu.disa.mil/recmgt/*.

The DoD database

Records Managers can use the sample DoD database included with IBM DB2 Records Manager to help them prepare their electronic record management information system to comply with the DoD 5015.2 standards.

The sample DoD database is contained in a package of XML files containing the File Plan and Component information. This required information lets you construct a complete sample database that contains the necessary information for completing the DoD tests. You can install the data using the IBM DB2 Records Manager Import Export utility. For information about importing data using the Import Export utility, see the *IBM DB2 Records Manager Import Export Guide*. The sample database files are located in */Toolkit/DoDSampleFilePlan*.

The sample DoD database provides you with a default file plan structure. This is a sample file structure used by records management offices and can be used to assist you in the certification process only. You must ensure that the database meets your requirements; it is not a final and complete database. It is a template to assist you with the certification process.

For more information, see the IBM DB2 Records Manager Toolkit, and the Records Management Application Compliance Testing Program located at *http://jitc.fhu.disa.mil/recmgt/*.

DoD Logic Extensions

IBM DB2 Records Manager logic extensions are necessary for developing a DoD compliant database. Logic extensions let you add custom logic to selected file plan component methods. Application developers can modify the behavior of the IBM DB2 Records Manager business objects, providing flexibility in the business model.

IBM DB2 Records Manager uses a simple listener pattern for each business object to modify. The logic extension files are located in */DoDLogicExtensions*.

For more information about logic extensions, see "User defined business logic" on page 8. For additional information about logic extensions, see the IBM DB2 Records Manager Toolkit, and the *IBM DB2 Records Manager Installation Guide*.

Outlook Extensions

The IBM DB2 Records Manager provides a seamless electronic records solution for Microsoft Outlook 2000. You can file an email message and its attachments as:

- A single record
- A separate record (linked)
- Both as a single record, and each attachment as a separate record (linked)

The Outlook Extensions contain modules for storing and describing email contents and attachments in the selected location. The application requires that all necessary file plan definitions and relationships be created before using the application. The Outlook extensions work through SOAP and require the Microsoft **.NET** Framework.

You must manually install the IRM DB2 Outlook email macro into Outlook 2000. For more information about this macro, see Chapter 5, "IBM email Module for Microsoft Outlook," on page 53and the *IBM DB2 Records Manager Deployment Guide* in the Toolkit.

The Outlook extensions lets you do the following:

- Declare email messages as corporate records
- Classify information, either manually or through an auto-classify rule
- Store the email and all its attachments in the corporate repository

For more information, see the Records Management Application Compliance Testing Program located at *http://jitc.fhu.disa.mil/recmgt/*.

Chapter 3. Designing a DoD 5015.2 Compliant Solution

This chapter describes how to build a “hybrid” solution consisting of both the host application and the DB2 Records Manager web administrator. This approach allows a solution to be built much more quickly because the existing web administrator interface is utilized for all records administration. Partners may decide to replace the web administrator interface by embedding this functionality into their own host administrator. There is nothing that is done in the web administrator that cannot be done in the host application using the DB2 Records Manager API. This approach simply takes more time.

If you want to build a solution that is certified compliant with the DoD 5015.2 standards for electronic records management, you have to provide some additional functionality in your solution beyond the “eRecords enabled” solution requirements. This chapter describes those requirements, and how you can meet them.

Note: This document discusses one approach to meeting the requirements; however, you may want to take a different approach. The requirements can be met in many different ways; there is no single correct way to meet these requirements.

About the requirements

There are two documents that outline the DoD 5015.2 requirements, and describe how to meet them: the DoD 5015.2 baseline requirements document, and the DoD 5015.2 test cases. Both of these documents are available on the DoD web site, located at *http://jitc.fhu.disa.mil/recmgt/*.

The DoD 5015.2 test cases describe the specific scenarios that the DoD testing team will run against your solution to confirm compliance. The IBM DB2 Records Manager Administrator Client (Web) satisfies many of these test cases. This document describes how you must change your application to meet the remaining test cases for your host.

The topics in this chapter describe the specific features you must provide in your host application to meet the DoD 5015.2 requirements (according to the DoD 5015.2 test cases). This walkthrough identifies all of the requirements satisfied by IBM DB2 Records Manager, including those that are not relevant to designing your integration with IBM DB2 Records Manager. It describes the work that must be done by the host application to ensure compliance. Under each test step, or group of test steps within the test case, you will see text in the following phrase:

The quick brown fox jumps over the lazy dog.

This text was extracted from the original test case document, and it will help you prepare for the test by explaining what you must do to pass the specific test. Whenever a specific test case or test step is extracted, there is an explanation describing the application (IBM DB2 Records Manager or your host application) responsible for carrying out the test. Where your application is responsible for carrying out the test, specific examples and instructions are provided. For information that describes who is responsible for satisfying each of the DoD 5015.2 requirements, see “DoD 5015.2 Requirements Summary for Partners” on page 27.

Because you are integrating your product with IBM DB2 Records Manager, you are required to write software code. This document provides you with useful insight to help you design and write your integration with IBM DB2 Records Manager.

Note: For many test cases, the test is self-describing and we have only provided additional comments.

Integration strategy

There are many strategies that you can use to integrate your product with IBM DB2 Records Manager; however, this document illustrates the following strategy:

- IBM DB2 Records Manager has no mechanism for storing electronic documents. It is designed to allow other applications to become eRecords-enabled, while allowing them to continue to focus on their core solution (and not records management). Your application will continue to be the host for all the documents and records, and you will "register" your documents as records with IBM DB2 Records Manager.
- IBM DB2 Records Manager provides users with a single point of login (using a common user account and password) with their "home" (typically the host) application. All user and group management functions will continue to reside within the host application. Users and groups are managed within the host application, and proxies for those users are created within IBM DB2 Records Manager. There is no need to specify duplicate users and groups in both of these applications. This is discussed in detail in "TEST SECTION 3: User Management" on page 12.
- All records related meta data is stored and managed using IBM DB2 Records Manager. The existing document related meta data in the host application does not require significant change; you must add a field to store the unique record IDs for any document declared as a record.
- All document filing templates and profiles are managed using IBM DB2 Records Manager. The host is responsible for rendering those profiles and applying those templates whenever a user in the host application declares a document as a record (you can use the IBM DB2 Records Manager API to obtain the document profiles and templates). The user can then provide the relevant records' related meta data, or the data can be retrieved from corresponding fields in the document meta data from the host.
- A key aspect of declaring a document as a record is to identify the file (also called record series) to which the record belongs. IBM DB2 Records Manager provides extensive functionality in its API for navigating the file plan; however, the host must provide a user interface that supports the ability to list only the file codes for which a user has filing access.
- You must also impose the same security regime on a document in your host application as the corresponding record profile in IBM DB2 Records Manager. This means that if a record profile in IBM DB2 Records Manager is designated to have a restricted access for a small group of users, the corresponding document in the host will likewise be restricted. The rationale for this approach is as follows: the DOD 5015.2 standard for records management application (called the **Standard**) mandates that access to records be restricted based on the record category or record folder in which they reside. Because the record category only exists in IBM DB2 Records Manager, that is where security is applied and is inherited by all records under it. If you do not implement this approach, your application might grant unauthorized users access to records in the host to which they do not have access in IBM DB2 Records Manager.

- The host application must create an implementation of the **HostInterface** and **HostServiceInterface** interfaces, and register the implementations with IBM DB2 Records Manager. For more information about these interfaces, see the online API Reference.

The DoD enabled database[1] for IBM DB2 Records Manager’

To save time and effort when configuring the necessary data for performing the required tests, you can install the DoD enabled database for IBM DB2 Records Manager’ (included in the Toolkit). This database consists of the following file plan views:

- DoD 5015.2
- Cross Reference
- Enclosures-Enclosure To
- Rendition
- Superceded - Superseding
- Supporting - Supported Documents
- Set View[2]

It also consists of the following file plan component definitions:

- Series
- Record Categories
- Folders
- Documents
- Email

File Plan Views: DoD 5015.2

This view is hierarchical and represents the file plan view that organizes the main objects that comprise the file plan. These include the following file plan component definitions: Series, Files, Folders, and Documents (described below). Included in the descriptions are the file plan component definition ID’s for each of the main types of objects. You need to know about these ID’s when writing your programs using the IBM DB2 Records Manager API.

Series	The broadest category of classification. In the file plan design, Series have one relationship definition that relates them to Record Categories, where the Series is the Source (for example, the parent in a hierarchical view) and the Record Categories are the Targets (for example, the children in a hierarchical view).
Record Categories	The next level of classification. Record Categories can contain Folders, Documents or Email. Record Categories have three possible relationships where the Record Category is the Source. Record Categories (as the Source/Parent) can be related to Folders, Documents, or Email (as the Targets/Children).
Folders	Represent mechanisms for organizing documents within a Record Category. Folders can contain documents and email, supporting two relationship definitions: a folder (as the source/parent) can be related documents, or emails (as the targets/children).

---

[2] To understand the concepts of file plan views and file plan component definitions, it is highly recommended you first read the *DB2 Records Manager Concepts Guide* before you continue with this document.

Documents	Represent the actual records. When a user from the host application “files” a document, your integration will create a new “document” in the file plan, and link it to an existing Record Category or Folder. Documents are the lowest level of the file plan and there are no relationships defined below them.
Email	Represent a special type of record. When a user from the host application “emails” a document, your integration will create a new “Email” in the file plan, and link it to an existing Record Category or Folder.

File Plan Views: Cross Reference, Enclosures-Enclosure To, Rendition, Superceded - Superseding, and Supporting - Supported Documents

Throughout the test cases discussed in this guide, records can be linked to each other to indicate some form of relationship. For example, in one test case, “supporting documents” are filed and “linked” to each other. This file plan view is added to accommodate these circumstances. It is a non-hierarchical view consisting of one relationship definition where Documents can be “cross referenced” to each other.

Set View

The Set View represents Document Versions. There are a number of test cases where a version of a document must be filed or retrieved. The Set view creates an ordered set of relationships between components of the same type. This type of relationship satisfies the requirements for linking and incrementing versions.

User defined business logic

This section is based on Revision 7.5 (May 2004) DoD 5015.2-STD RMA COMPLIANCE TEST PROCEDURES. The basis of several test cases come from the following requirement in the DOD 5015.2 Design Criteria Standard For Electronic Records Management Software Applications. This requirement is as follows:

> *C2.2.1.5. RMAs shall provide the capability to allow only an authorized individual to define and attach user-defined business rules and/or access logic to any metadata field including user-defined fields.*

Logic extensions and J2EE client applications provided by IBM

IBM provides you with the following logic extensions:

- “IRMDocumentExtension.jar”
- “IRMDodReportClientEAR.ear” on page 9

IRMDocumentExtension.jar

The *com.ibm.gre.dod.extension.DocumentListener* class is contained in the file *IRMDocumentExtension.jar*, included in the Toolkit folder. (See: Toolkit\DoD 5015.2\DoDLogicExtensions\LogicExtension.)

This is a logic extension that you must install into the IBM DB2 Records Manager Extensions facility for the Document file plan component. For details on how to create and edit logic extensions in IBM DB2 Records Manager, see the *IBM DB2 Records Manager Records Installation Guide*. This logic extension contains the special logic attached to the “Project” field. It runs each time a document is added or updated, and it updates the Access Control List for the document based on the document’s original Access Control List and the “Project” field. It also sends a notification Email when a record is superseded in a category that has a final disposition of “Destroy when superseded or obsolete”.

For configuration details, see the *readme.txt* file that is included with this extension.

This same Extension is also required for the Email file plan component.

IRMDodReportClientEAR.ear

This J2EE Client Application adds logic to send an email to a specified user when a vital record folder is due for review, It adds user-defined logic to the user-defined field Project to generate an end of day report containing records ordered by project name, and identifies who has access to those records.

There are two batch files called *projectAccess.bat* and *vitalRecords.bat* that can be executed directly to run the reports.

During the testing phase

Testing the special logic associated with the field named “Project”

There are two special tests for this field. The first test involves the Access Restrictions placed on a document based on its assigned project. At the beginning of the test case, ensure that the Document extension and the Email extension are enabled. These extensions occur every time a document or email is added or updated. These extensions update the ACL assigned to each document based on the document’s original ACL, their assigned Supplemental Markings, and their Assigned Projects.

The second test involves the generation of a special report: “Add user-defined logic to the user-defined field Project Name” (Generate an end of day report of records ordered by project name and who has access). You perform this test by running the *projectAccess.bat* file.

Testing the special logic associated with vital record review

To test this case, you can run the file called *vitalRecords.bat*to send an email (to the configured user) when a vital record folder is due for review.

DOD 5015.2 test cases

TEST SECTION 2: Test Readiness Evaluation

Evaluate Set-up

This topic provides testers with insight into your readiness for the testing process. Previously, the DoD testers have encountered situations where they have stopped the test and failed the vendors due to the vendor’s lack of readiness. IBM DB2 Records Manager helps towards your preparation by providing a pre-built file plan, users, groups, profiles, and defaults that you can use for your certification. These are available in the Toolkit. You can also use your own users and groups, and document profiles within your own application (such as forms used to capture document and record meta data). You must have the features described here-in built and ready to demonstrate your readiness for the test.

Verify user accounts: The IBM DB2 Records Manager's DoD-ready database includes predefined user, however they are considered LOCAL groups. If you want to use your own groups, you must ensure that these groups are defined in your host, and that they have been imported into IBM DB2 Records Manager.

For a list of user accounts used during testing, see the Test Cases Document.

Verify Groups: The DB2 Records Manager's DoD-ready database includes predefined groups, however they are considered LOCAL groups. If you want to use your own groups, you must ensure that these groups are defined in your host, and that they have been imported into IBM DB2 Records Manager.

For a list of these groups, see the Test Cases Document.

Verify standard data elements: For a pairing, verify that these elements are set up in the host application (Document Management, Work Flow, and so forth), and that they are properly mapped to the RMA.

The host application is only responsible for standard data elements related to documents. Standard data elements related to file plan components and folders is the responsibility of IBM DB2 Records Manager. You must ensure that your application either provides these fields and maps them directly to IBM DB2 Records Manager, or upon declaration of a record, that you provide a data entry form allowing the user to provide the information to IBM DB2 Records Manager.

For a list of the standard data elements, see the Test Cases Document.

Verify Groups: Verify the data entry templates. For a pairing, verify host system data entry templates provided by the IBM DB2 Records Manager DoD-ready database. Your host application, must provide the ability to RENDER *Electronic Record* templates when a user declares a document as a record with IBM DB2 Records Manager.

For a list of the data entry templates, see the Test Cases Document.

Verify the file plan: The necessary file plan components are included in the IBM DB2 Records Manager's DoD-ready database.

Verify Access and Limitations: The Test Cases Document outlines four types of access limitations:

1. Restrictions on the users ability to file records into portions of the file plan.
2. Restrictions on the groups ability to file records into portions of the file plan.
3. Restrictions on the users ability to search for, and retrieve records from, portions of the file plan.
4. Restrictions on the groups ability to search for, and retrieve records from, portions of the file plan.

The permissions are described in detail in four separate tables in the Test Cases Document.

The necessary permissions are specified in the IBM DB2 Records Manager' DoD-ready database. However these permissions are specified for the pre-defined local users and groups only. If you want to use your own host users and groups, you will need to apply these permissions for your groups as well.

Negative Testing

Attempt to access the functions to manage users.
Attempt to access the functions to manage groups.

Because user and group management occurs in the host application, these tests are also performed in the host application, and some of these tests are performed in IBM DB2 Records Manager. These tests include those related to assigning records-specific permissions (permissions that have no relevance in the host application).

Attempt to access the functions to change standard data element mapping/definition.

All records related data elements exist in IBM DB2 Records Manager, therefore these tests will occur in IBM DB2 Records Manager. If some data elements are defined within your host application, these tests can be performed within the host application. Your host should have the ability to restrict access to these functions.

Attempt to access any functions to create/modify control tables or global lookup lists.

Control tables and lookup lists are related to data elements for records. Because these exist only in IBM DB2 Records Manager, these tests are performed there.

Retrieve a record, attempt to modify the content, attempt to modify the meta data, attempt to change the folder/record category. (The user should be allowed to enter event dates to the meta data.)
Attempt to change the meta data of a filed record. (As a privileged user, should be allowed to add event dates to Event/Time-Event folders.)

The record content is stored in the host application. It is therefore the responsibility of the host application to ensure that **under no circumstances** can the content of the record be altered.

Note: Any host-specific document meta data is considered record meta data and is subject to the same permissions as the IBM DB2 Records Manager-specific record meta data. It determines whether a specific user is allowed to alter the record meta data, an whether they can access the ACL (access control list) of the record from IBM DB2 Records Manager. For additional information, see **FilePlanComponentControllerEJB.getEffectiveUserPermissionsList** in the *IBM DB2 Records Manager API Reference*. If your host maintains its own ACL, IBM DB2 Records Manager can automatically inform it whenever permissions change that affect one or more documents stored in your host. At that time, the host can automatically update its own ACL.

Attempt to file a record. Note what categories/folders are visible. Verify that only current and valid record categories or folders are available to the user/workgroup for filing.

When filing a record, the standard requires that only files to which the user has access to file documents are visible. When filing documents, there is no need to show a user files to which the user does not have the permissions to file documents. There are many approaches that can be taken to meet this requirement.

A sophisticated approach is to query each file to determine whether the user has permissions to file documents within it, and if not, to not include the file in the file plan hierarchy of the navigator. The IBM DB2 Records Administrator Client interface uses this approach. If you create your own navigator, you can use the IBM DB2 Records Manager API function called **filePlanComponentControllerEJB.getEffectiveUserPermissionsList** to obtain the set of permissions a particular user has for a file.

To learn more about the concepts related to file plan design, see the *IBM DB2 Records Manager Concepts Guide* and the *IBM DB2 Records Administrator's Guide*.

Attempt a "select all" search. Note what categories/folders are returned.

If your host application has its own search facility, you must also impose the same security regime on a document in your host application as the corresponding record profile in IBM DB2 Records Manager. Otherwise, your host application might grant users access to documents that they should not see. You can use any of the following methods to obtain the permissions for a document for a particular user:

- **filePlanComponentControllerEJB.getAllowedHostActionList**
- **filePlanComponentControllerEJB.getAllowedLocalActionList**
- **filePlanComponentControllerEJB.getEffectiveUserPermissionsActionList**

For details about these functions, see the *IBM DB2 Records Manager Programming Guide* and the *IBM DB2 Records Manager API Reference.*.

This approach assumes that prior to showing a user the results of any search, you will query IBM DB2 Records Manager for each record to determine whether it can be shown. This may not be feasible if the number of records returned in result lists is large, or if system performance is critical. Alternatively, you can synchronize your record's ACL with the one in IBM DB2 Records Manager.

IBM DB2 Records Manager now uses “On Demand Synchronization”. Host applications that want to synchronize ACLs can call the **BatchControllerEJB** to run an asynchronous task, requesting all changes affecting the host application records. For more information about **BatchControllerEJB**, see the API Reference.

Attempt to create and maintain shortened "quick-pick" lists from the authorized lists. (The user should be allowed to do this.)

You can test the maintenance of shortened quick pick lists (which are user specific subsets of master pick lists) using IBM DB2 Records Manager; however, your host must be able to RENDER quick pick lists. For information about pick lists, see the *IBM DB2 Record's Administrator's Guide*.

Attempt to create and maintain templates with default values. (The user should be allowed to do this with their own templates, not organization-wide templates.)

Typically, the creation and maintenance of data entry templates and defaults occurs in IBM DB2 Records Manager. Therefore, this test can be performed there, but the host application must be able to RENDER those templates and apply the defaults within its own application

TEST SECTION 3: User Management

Create User Accounts

IBM DB2 Records Manager lets you use your own users and groups defined in your host application as the users and groups within IBM DB2 Records Manager. You can use IBM DB2 Records Manager to create proxies of your application user and group accounts, and to grant those proxies explicit permissions to perform actions within IBM DB2 Records Manager. This means that you can manage your users and groups in one application (not two). It does not require you to have separate user login names for each application.

This document assumes that user and group management is performed within your application, and that only proxies of your application's user and group accounts are added to the IBM DB2 Records Manager database. This means that you would have implemented the **getGroupsList** and **getUserList** functions in **hostInterface**.

Note: Any application integrating with IBM DB2 Records Manager must implement the **hostInterface** and register it with IBM DB2 Records Manager.

For details about **hostInterface**, see the *IBM DB2 Records Manager API Reference*[3], the *IBM DB2 Records Manager Technical Reference*, and the *IBM DB2 Records Manager Programming Guide*.

After you add a proxy for a user account to the IBM DB2 Records Manager database, that user can access IBM DB2 Records Manager features directly from within the host application. They must log on to IBM DB2 Records Manager; however, they can be logged on using a special function belonging to the **LoginManagerEJB** class (from the IBM DB2 Records Manager API). This function, called **hostLogin**, assumes that a user logs on from the host application, and that this user is valid in the host application.

A user with a proxy in IBM DB2 Records Manager can also directly log on to IBM DB2 Records Manager. That user must provide their credentials, and the host application to which they belong, to IBM DB2 Records Manager. IBM DB2 Records Manager uses these credentials to validate the user with the host application before granting the user a session.

Because the host application performs the user and group management, you will add users and groups into the host application. Next, you will "import" them into IBM DB2 Records Manager. To import your users and groups, for your application you must implement the **getUserList** and **getGroupList** methods from the interface called **hostInterface**. For information about **hostInterface**, see the *IBM DB2 Records Manager API Reference*.

After you implement this interface, you can use IBM DB2 Records Manager to directly import your users. For instructions about how to import users, see the *IBM DB2 Records Administrator's Guide* and the *IBM DB2 Records Manager ImportExport Guide* for instructions on how to import users).

In IBM DB2 Records Manager, the **Supplemental Markings** field controls access to records (used in the user and group profiles in conjunction with the IBM DB2 Records Manager' macro facility). You must provide the **Supplemental Marking** values to the user's profile in IBM DB2 Records Manager **after** you import the users from the host application.

You can delete a user account from within the host application, and programmatically delete the corresponding proxy in IBM DB2 Records Manager using the IBM DB2 Records Manager API. You can call the method **getUserByExternalUserId** within **UserControllerEJB** to the obtain the user's IBM DB2 Records Manager ID, and then call the **deleteUser** method to the delete the user.

However, if you do not delete the proxy from IBM DB2 Records Manager, the user will no longer be able to log on to the host application, and so will not be able to access IBM DB2 Records Manager using the **LoginManager.EJB.hostLogin** method. Although the proxy remains in IBM DB2 Records Manager, the user will not be able to log on to IBM DB2 Records Manager because IBM DB2 Records Manager will first validate the user's 'credentials with the host application. Because the host user account was deleted within the host application, the user does not validate and IBM DB2 Records Manager will not allow the user to complete the login process.

---

[3] NB - For this mechanism to be successful, the host application must provide a unique immutable identifier for each user and group. This immutable identifier "points" IBM DB2 Records Manager to the actual account in the host application. The Login Name or User Name cannot be used if they are not immutable.

Note: You must implement the **hostInterface.ValidateUser** method so that the method accepts the user's valid credentials, and validates the user against the host's database. If the user does not validate, this method must return an empty string; otherwise, it must return the user's Immutable ID. If this ID has a corresponding proxy in the IBM DB2 Records Manager database, IBM DB2 Records Manager will grant the user a session.

Attempt to log on using 'an old password. Verify that logon is unsuccessful.

Because the host application performs user and group management, modifying user accounts also occurs within the host. Within IBM DB2 Records Manager, there is only a proxy for the real account. It does not store a login ID or a password. This proxy is immutable and there is no need to re-synchronize accounts between the host and IBM DB2 Records Manager (greatly reducing the complexity inherent in maintaining separate user accounts in two applications). To automatically change the login ID and the name (programmatically) when a change occurs in the host, you may want to extend the integration between IBM DB2 Records Manager and your host application. Otherwise, these can be changed manually by an administrator in IBM DB2 Records Manager.

Generate a printed listing of all users for reference during the test. Verify the printed output against the expected results.

If the host application allows the printing of users and groups, you can complete this test step using the host application. Otherwise, you can generate a user report for the user proxies using the IBM DB2 Records Manager reporting facility.

Create User Groups

IBM DB2 Records Manager treats users and groups in the same way. For details on creating groups in the host application, and creating proxies for the users in IBM DB2 Records Manager, see the discussion (above) related to users.

This document assumes that all user-group membership is maintained in the host application. IBM DB2 Records Manager supports the management of host users and groups within the host application, and to incorporate the user-group membership when the user logs in. Every time a host-based user logs on, whether by logging on directly to IBM DB2 Records Manager or by logging on from the host application using **LoginManagerEJB.hostLogin**, IBM DB2 Records Manager queries the host application to provide a list of groups to which the user belongs. IBM DB2 Records Manager creates a temporary user-group membership between the user logging on, and each group to which the user belongs. This temporary membership expires after the user logs out. This means that host applications can assign users to groups without regard for IBM DB2 Records Manager, and that when the user accesses IBM DB2 Records Manager features, they will have the rights and permissions from all groups to which they belong.

When a user logs on to IBM DB2 Records Manager from the host application, the **hostLogin** method of the **LoginManagerEJB** class is used (IBM DB2 Records Manager API). One of the parameters in that method is the Group List to which the user belongs. For details about the **LoginManagerEJB** class, see the *IBM DB2 Records Manager API Reference*.

When a host user logs on to IBM DB2 Records Manager specifying the Host Name, the user is only required to provide their valid credentials. After IBM DB2 Records Manager validates the user's credentials (using the **validateUser** method from **HostServiceInterface**), IBM DB2 Records Manager calls upon the host to provide a list of groups to which the user belongs. For descriptions about the **HostServiceInterface** interface, see the *DB2 Records Manager API Reference* .

Note: While IBM DB2 Records Manager supports the management of users and groups and user-group membership, when paired with another product that has its own user and group management, it is important that care be taken when host users (their proxies) are assigned to host groups (proxies) using IBM DB2 Records Manager user-group management. Doing so will create user-group memberships outside of the host application that may not exist in the host application. Unless you use the API to show these relationships, they will not appear in the host application.

Because the host application performs user and group management, you will add users and groups into the host application. You will then "import" them into IBM DB2 Records Manager. For your application, to import your users and groups, you must have implemented the **getUserList** and **getGroupList** methods from the **HostInterface** interface. For information about the **HostInterface** interface, see the *IBM DB2 Records Manager API Reference*. After you implement this interface, you can use IBM DB2 Records Manager to directly import your groups. For instructions about how to import groups, see the *IBM DB2 Import Export Guide* and the *IBM DB2 Records Administrator's Guide*.

Functional Access within the context of this certification means access to features in IBM DB2 Records Manager. After Groups from the host application are imported into IBM DB2 Records Manager, assigning functional access is performed within IBM DB2 Records Manager. Members of the Group can then directly log on to IBM DB2 Records Manager to test functional access.

Generate a printed listing of all groups for reference during the test. Verify the printed output against the results, based on the previous steps.

If the host application allows the printing of users and groups, you can complete this test step using the host application. Otherwise, you can generate a user report for the user proxies using the IBM DB2 Records Manager reporting facility.

TEST SECTION 4: Set up File Plan

Build the File Plan Infrastructure

IBM DB2 Records Manager is an API with a user interface. You can use this API to embed all IBM DB2 Records Manager features necessary to complete this test case within your host application. The benefits of this approach is that you will provide your customers with a seamless, single user interface.

However, IBM DB2 Records Manager also provides a Web-based user interface that lets you perform these functions and meet the requirements of this test case without having to retrofit your existing application.

One aspect of building a file plan infrastructure involves the creation of data entry templates and default values for data entry when filing a document. Because filing a document involves a user operating in the host application and filing the record with IBM DB2 Records Manager, you must provide a mechanism for rendering the data entry templates and populating those templates with predefined default values. If your application is Web-based, you can use the IBM DB2 Records Manager' profile rendering mechanisms (for setting the default values).

Because the management of file plans is strictly a records management function, something for which IBM DB2 Records Manager is designed, this document assumes that you use the IBM DB2 Records Manager Web-based user interface to build the file plan infrastructure, and to perform the test in this section.

For detailed instructions about the remaining test steps in this test case, see the relevant sections in the *IBM DB2 Records Administrator's Guide*.

A significant change to Version 6.6 of the test cases is the inclusion of user defined logic on several fields in IBM DB2 Records Manager. This change is based on the following requirement in the DoD 5015.2 Design Criteria:

> C2.2.1.5. RMAs shall provide the capability to allow only an authorized individual to define and attach user-defined business rules and/or access logic to any metadata field including user-defined fields.

This includes the field named **Project**; a custom defined field in IBM DB2 Records Manager. Throughout the test cases you will find references to user defined logic attached to this field. We have gathered all the references from the document and included them here (part of the infrastructure of the file plan). The infrastructure of the file plan is the user defined business logic that extends the functionality of IBM DB2 Records Manager.

To help you pass these test cases, IBM has developed a number of logic extensions and J2EE client applications. For more information, see "Logic extensions and J2EE client applications provided by IBM" on page 8.

Create/Maintain Record Categories and Folders

These test steps can be completed using the IBM DB2 Records Manager user interface. For details about how to carry out these steps, see the *IBM DB2 Records Administrator's Guide.*.

Limit Record Categories and Folders

These test steps can be completed using the IBM DB2 Records Manager user interface. For details about how to perform these steps, see the sections in the *IBM DB2 Records Administrator's Guide,* about applying permissions to file plan components.

TEST SECTION 5: Filing

These test cases comprise the essence of the integration between IBM DB2 Records Manager and your application (the host). To be certified in a product pairing, you must demonstrate your application's ability to support these test steps in conjunction with IBM DB2 Records Manager.

The nature of product pairings is that host application users are logged onto the host application doing normal business functions. The host application must therefore support the ability of a host user to declare a document managed by the host system as a record.

The normal user procedures for filing a record (there are many variations) from within a host application are as follows:

The user is logged into and working within the host application.

The user identifies a document to be filed as a record.

The user clicks on a button inserted into the host application that will launch a middleware utility. This utility will present to the user a "file plan browser" allowing them to navigate the file plan constructed in Test Section 4.

The user will navigate the file plan and identify a file (record category) into which the document will be filed.

This utility will also present the user with a record filing profile. The user must supply records specific profile information (see below for what must be supplied on the record profile).

The user will enter the information and click OK.

This document assumes that you will provide the mechanisms for rendering the data entry profile (item 5) based on the data entry templates created in Section 4, and that you will provide the mechanism for navigating the file plan (item 4). These are illustrated elsewhere in this Guide. If your product is web based you can use the corresponding mechanisms that are part of the DB2 Records Manager off-the-shelf user interface and embed the JSP pages into your application.

You must also provide a mechanism for logging the current user into DB2 Records Manager using the Login function so that they may file their document.

FILE ELECTRONIC DOCUMENTS

Four users log on the RMA (for pairings, log into the host application) as show below. All four users will work simultaneously to file documents, as indicated in the following four steps.

It is assumed that these users will be logged into the host application and will be registering their documents with the DB2 Records Manager.

The following table identified the fields added as user defined fields in the DoD enabled database for IBM DB2 Records Manager: Supplemental Marking (Security Descriptor) List, Media Type, Format, Publication Date, Date Received, Author/Originator, Originating Organization, and Record Location. If you do not intend to use the DoD enabled database, you will need to create these fields yourself using the IBM DB2 Records Manager Custom Field creation mechanism.

Table 1. DOD 5-1.1—Editing Permissions for Record METAData — During Filing

Metadata Field	Indicate Auto-capture or Manual Entry	Editing Allowed?
Media Type		
Format		
Date Received		
Author or Originator		
Addressee(s)		
Other Addressee(s)		
Originating Organization		
Location		
User-Defined Fields		

This document assumes that all records related meta data in the above table will exist in the IBM DB2 Records Manager database. Some of these fields may already exist in the host application. DoD testers look for an automatic mapping of these field values into the corresponding fields in theIBM DB2 Records Manager records meta data. While this is acceptable from the standpoint of the test procedures, it may be difficult to keep the data in the two applications the same.

Note: From the standpoint of the Standard, the two applications in concert form a single solution. It does not matter in which of the two applications the fields reside, as long as they are easily accessible from a single user interface, they can show up in a single "record" profile, and they can be incorporated into report queries (see Test Section 6) You may choose to avoid duplication of fields between the two applications so long as you provide a single point of access for the "complete" metadata you support the inclusion of both sets of meta data in a report.

The easiest solution is to capture all records related data in IBM DB2 Records Manager, and to use its meta data rendering (profiles) and reporting features to meet the requirements of the Standard. It is this solution that is assumed in this document.

Verify all user-defined fields are on filing screen.

The creation of user defined fields is supported by IBM DB2 Records Manager. After the fields have been defined, they must be included in a user define filing template in order to be rendered to the user. It is then the responsibility of the host application to render the profile when a user files a record.

File at least one document with multiple categories.

A "category" corresponds to the DB2 Records Manager File object. You must demonstrate the ability to register a single document more than once under a separate File. Each time you register the document as a record, IBM DB2 Records Manager will create a new record entry with its own Unique Record Identifier. All record entries, however, will point back to the same document in your host application. You must, however, record the Unique Record Identifier for each new record that you register with DB2 Records Manager. A single document in your Host Application may have more than one Unique Record Identifier.

During daily processing, DB2 Records Manager may instruct the host to Delete a particular document. In addition, during disposition processing, DB2 Records Manager will instruct the host to TRANSFER, DESTROY or ACCESSION that document. The Host application must ensure that the document is **not** deleted if that document has more than one Unique Record Identifier. It must instead remove reference to that Unique Record Identifier. Only when a document is reduced to the last Unique Record Identifier can the document actually be deleted from within the Host's repository.

There are two approaches you can take. The first is to record all the Unique Record Identifiers related to a single document within your application. The second approach, if this is not feasible given your application's architecture is to use the **FilePlanComponent.ControllerEJB.getAllowedHostActionList** method. While not originally intended for this purpose, it provides a convenient way to get a list of all Unique Record Identifiers (File Plan Component ID's) for any particular document stored in the host application. Passing it in your document id (the external record id as defined in the DB2 Records Manager), you will receive a list of all file plan component ID's related to the document ID.

Another factor you must consider when you implement your solution around this requirement regards the security regime that will apply to any document registered under multiple categories. Such a document could conceivably inherit different access control lists from different branches of the file plan. Which is the correct one? One approach is to create a virtual access control list which is the intersection of the separate access control lists. Such an access control list ensures that a user must derive any specific permission from all access control lists in order to be able to carry out the function related to the permissions. For example, in order to be able to VIEW a document, a user must be able to VIEW that document in all the access control lists from the different branches in the file plan.

If you are using the DB2 Records Manager API to determine in real time what are the permissions allocated to a user for any particular document, you can use the **FilePlanComponentControllerEJB.getAllowedHostActionList** method. This will return a complete list of permissions allocated to any user for all occurrences of any document in the file plan.

If, however, your implementation is updating the document's local access control list in the host from the access control list of the document's corresponding file plan component entry in the DB2 Records Manager you must adopt the following approach.

This approach will only work if you have also implemented a Message Driven Bean that is capable of receiving Security Notification Events and Permission Synchronization events.

1. Implement a Message Driven Bean that responds to Security Notification Events and Permission Synchronization events.
2. Monitor the Security Notifications and Call **BatchControllerEJB.beginTask - AsynchronousTaskType.PERMISSIONS_SYNCHRONIZATION** when you determine that a sufficient number of changes have occurred to warrant synchronization. This method will begin a batch process that will eventually return a list of file plan components in your host whose permissions were changed. For more information on this process see the *IBM DB2 Records Manager API Guide* and *Programmers Guide*.
3. Using the information supplied for each Item in this list the Host Application can synchronize it's security attributes with the Records Managers attributes.

Designate at least one document as a vital record and add the monthly review dates.

Vital Record indicator is a Core field on all File plan component profiles. You must, however, ensure it is included in any document filing profiles in order for it to be rendered to the user from your host application.

File supporting documents, indicating they are linked, specify the relationship.

There are numerous ways to meet this requirement. The simplest is to use the concept of file plan views as it is supported by DB2 Records Manager. However, before you proceed, it is highly recommended that you read the *DB2 Records Manager Concepts Guide* related to file plan views and file plan relationships.

The DB2 Records Manager DOD 5015.2 enabled database supplies you with the necessary structure. In it you will find a non-hierarchical view named "Cross Reference". This view supports one relationship definition that allows documents (records) to be related to each other in a non-hierarchical fashion. In DB2 Records Manager, you can "relate" one document to another by creating a relationship between two documents within the cross reference view. The view provides the context of the relationship, in this case this is a Cross Reference relationship between two documents.

You can use the existing features in the DB2 Records Manager off-the-shelf user interface to view those relationships.

File superseded/superseding documents, indicating the relationship.

Superseding a document may cause the life cycle of the superseded document to commence. You will find many disposal instructions stating "Destroy when superceded" or "Destroy 10 years after the record is superceded". A record commences its life cycle on the date specified in its life cycle date. The DB2 Records Manager wraps up the necessary functionality to commence the life cycle of a record in a single function: filePlanComponent.Supersede.

In order to illustrate this test, you must file a document as a new record, locate an existing document and indicate that the new document supersedes the existing document. You must then create a relationship between the superseded and the superseding document. A simple approach is to place a "Supersede" button on the filing profile you choose to render. If a user is filing a document and they wish the new record to supersede an existing record, clicking on the supersede button will launch a file plan explorer allowing them to selected the superseded document. You can then call the filePlanComponent.Supersede method for the superseded document. Finally you can create a relationship between the superseded and superseding document. You should however create a new view to support the superseding relationship or you can use the existing Cross Reference View.

File multiple renditions of a document, verify linking and relationship.

A rendition is a separate physical representation of the same document. An example of two renditions of a document can be MS Word format and PDF format. DB2 Records Manager allows you to support multiple renditions within your host application and link those renditions to a a single unique record ID. It is the responsibility of the host to bundle the various renditions of a record. You can inform the IRM of the various renditions related to a record by implementing the method (getContentList) in the host interface.

File a new version of a record, verify incrementing and linking.

If your host application has a mechanism for supporting multiple document versions, you can simply file each new version of a document as a separate record in DB2 Records Manager. You must however, LINK the two records using SETS. The Set View allows records to be linked together in an ordered set. When a new version is added in the host system, you must add the corresponding record in the Records Manager as a new member of a SET. For more information on SETS see the IBM DB2 Record's Administrator's Guide.

If your host application does not support the concept of multiple versions you can employ some advanced concepts in DB2 Records Manager. To understand more about these concepts, please read the *DB2 Records Manager Concepts Guide*. In your host application, you can create a new document for each version of the record. Then, using the DB2 Records Manager's file plan design features add a new file plan component definition named VERSION as a sub-element in the DOD 5015.2 file plan to the existing document file plan component definition. This means that each document can be comprised of one or more versions in the file plan hierarchy. When you file a new document in DB2 Records Manager, if that is a new document, your integration will first create a new Document, then it will create Version 1 of that document as a sub-element of the document. For all subsequent versions, it will simply add the additional version to the existing document.

You can combine this technique to the technique described previously whereby a document is comprised of version and each version is comprised of renditions.

File Email Messages

The standard requires that any RMA provide a capability to capture email as records. Normally (though not necessarily) this entails moving or copying the email message and its attachments into the secure repository of the RMA.

Outlook extensions are part of the Toolkit.

The DB2 Records Manager provides you with a Microsoft Outlook 2000 plug-in that allows you to quickly build an email capture solution for the purposes of meeting the Standard. This plug-in is provided in the form of a macro and a COM DLL named IRMEmailModule.dll. You must extend the macro so that it copies any email and its attachments into your host application's repository. The locations of the Macro where you must add your code are well documented. The DLL provides a ready made rendering device for metadata capture forms and writes the metadata to the DB2 Records Manager. This assumes that all records related meta data will be stored in IBM DB2 Records Manager. If some meta data is actually to be stored in your host application you may not be able to use this DLL. You can instead write your own. For details consult the section in this guide regarding integrating your application with email.

Consult the relevant sections of the toolkit regarding email integration.

File Non-Electronic Documents

Unless you plan to record the profiles of external (non-electronic) documents into your host application, this test can be carried out exclusively within IBM DB2 Records Manager. This document assumes that you will use IBM DB2 Records Manager to file non-electronic records. For details on how to perform these test steps, see the *IBM DB2 Records Administrator's Guide.*.

TEST SECTION 6: SEARCHING FOR AND RETRIEVING RECORDS

Search and Retrieve

When designing your solution to meet the requirements of the Standard, you must also consider Searching. First, you must consider the requirements for searching when you apportion the fields that comprise the record metadata. In Test Section 5, we discussed possible scenarios for apportioning some records related fields in each of the applications. While this may reduce duplicate data, it may also make it very difficult to meet other requirements, such as searching. The Standard requires that you provide the ability for a user to construct queries based on any sub-set of the records related meta-data. This is least difficult to implement if all the metadata resides in a single application with a single reporting tool. If you choose to apportion all the records related metadata to DB2 Records Manager, then searching can be carried out entirely within DB2 Records Manager. This document assumes that you will be apportioning all the records related metadata to DB2 Records Manager. Therefore, these test cases can be carried out entirely by DB2 Records Manager (with the exceptions noted below).

There are two ways you can implement this solution. The most straightforward way is to have the user log on to IBM DB2 Records Manager using the IBM DB2 Records Manager login screen. The user can then execute the searches completely within DB2 Records Manager. However, they will be using the IBM DB2 Records Manager user interface which will probably differ significantly from yours. You must also implement the ability for users to retrieve the document from your Host repository. The normal user procedures for these tests are:

1. The user will be logged into DB2 Records Manager and will navigate to the report query screen.
2. The user will construct the query and select the output fields of the report.
3. The user will execute the report and receive the items matching the query in a formatted result list.

4. The user will identify a record to be retrieved and will select its properties form.
5. The user can then elect to retrieve one or more renditions of that record to the user's workspace.

See Chapter 4, "Summary of Requirements for Partners and What's New," on page 27 for a detailed description on integrating your product with DB2 Records Manager's reporting facility.

Note: Documents continue to reside in your host application. Which means they continue to be accessible by normal users from within your host application. The Standard mandates that access to records be limited based on the file (record category) to which the record belongs. You must therefore implement a mechanism whereby access control on any document declared as a record is levied onto your host application by the DB2 Records Manager. For example if a user in your host application executes a search within your host application (if your host supports searching), and the user does not have access to view records located in a particular location, then the result list within your application MUST NOT include any documents declared as records and filed in that location. The DB2 Records Manager has several methods that allow you to query on the security of any individual record. These methods include **getAllowedHostActionList** and **getAllowedLocalActionList**. Consult the *DB2 Records Manager API Reference* for details on these two methods. In addition the DB2 Records Manager provides a way to synchronize the access control list of your own document with the access control list of the corresponding entry in the DB2 Records Manager. For details, consult the section in this guide describing how to implement the HostInterface.

Retrieval of records occurs mostly in concert with searching for records. However, the records themselves reside inside your host application. If you intend to use the DB2 Records Manager off-the-shelf user interface to conduct all records related searching, you must provide an implementation that allows a user conducting a search to retrieve the separate record renditions to their workspace.

To allow a user to retrieve records from a host application, you must implement the following methods in the remote host interface
1. getContentList
2. openContentStreamForRead
3. readContentStream
4. closeContentStream

For details of these methods consult the API Reference. You must also configure your host to support retrieval of content in the host configuration form. Consult the IBM DB2 Record's Administrator's Guide for host configuration.

Integrating the DB2 Records Manager reporting and retrieval: If you have wrapped the DB2 Records Manager reporting API with your own user interface into your own Host Application, you can provide your own devices that best suit your needs.

You must insure that under no circumstances can a document within your Host application that has been registered as a record be modified. If the document is modified then the new version of the document must be explicitly declared as a separate record.

TEST SECTION 7: SCREENING AND EDITING RECORDS

Screen Records

The screening of records is a records management business function. The procedures in this test case are carried out using the DB2 Records Manager own features and user interface. For details on how to use the DB2 Records Manager to carry out these steps, consult the DB2 Records Manager User's Guide.

Reschedule Records

There are three methods to reschedule a record. All of which can be carried out using the DB2 Records Manager's own user interface without involvement of the host.

The first way is to move the file plan component corresponding to the record to a new file category with a different life cycle code. Because records inherit their life cycles (schedules) from their parent file categories, you have effectively re-scheduled the record. If, however, the host application is storing any information related to the file category, then the host MUST be updated separately. As an alternative, you could implement the MOVE functionality within the HOST by calling FilePlanComponentControllerEJB.setSource.

The second way is to allocate a different life cycle code to the record's parent file category code. This too will effectively re-schedule the record.

The third way is to modify the life cycle code. Altering the duration of a life cycle or changing the disposition effectively re-schedules any records to which that life cycle code applies.

Cycle Vital Records

Cycling of vital records entails reviewing individual vital records or the folders in which they reside to determine whether they are still vital. Each file plan component profile has a field name VITAL. If this is set, a record is vital. For any vital record you must also supply the last vital record review date, and the review period. Normal practice is to designate a folder as vital, indicating that any records within it are vital. Such a test would normally be carried out entirely in the DB2 Records Manager. However, a user may wish to review the actual content of a record to determine whether it is still vital. The host must therefore implement the ability to view the content of the record (i.e. to retrieve the record). See the section on the Search and Retrieval of records.

TEST SECTION 8: DISPOSITION MANAGEMENT

FOLDER CLOSING AND CUT-OFF PROCESSING

Closing and cutting off of record folders is carried out entirely within the DB2 Records Manager. These test steps are carried out using DB2 Records Manager.

DISPOSITION PROCESSING

The DB2 Records Manager will be responsible for managing all aspects of the life cycle of the each record. It will calculate when a record is to be disposed. The host application has the following responsibility: Because the host application is "hosting" the document, it must ensure that, when called upon by DB2 Records Manager during disposition processing, it will effectively "dispose" of any record stored in its repository.

There are two types of disposition that your host must support: Destruction and Accession.

Destruction is simply the irrevocable deletion of the record from your repository. Accession is the final MOVING of that record to another authority; effectively surrendering ownership (and legal responsibility for maintaining) the record.

Note: After a record has been accessioned, it must also be deleted from your host repository.

To meet these requirements, DB2 Records Manager has defined an interface that you must implement. The interface is named HostInterface and is found in the com.ibm.gre.engine.recordhost package. For details on this consult the appropriate section of this guide and also the *DB2 Records Manager API Reference*.

There is a third life cycle event that your host must handle. It is defined as an "Interim Transfer". An interim transfer is defined as the moving of a record to an external repository while still maintaining ownership of the record. For this situation, the record is removed from the repository, however the meta-data of the record is retained. While this applies more to paper records it has been tested for electronic records. In such a case your host implementation must know that a record has been transferred. If called upon to transfer or dispose the record again it should return a zero return code (no Error) but it must provide information in the return XML (see the HostInterface.phaseTransition method in the API Reference) that the record has already been transferred, and that the record resides elsewhere.

Ensure records filed into multiple record categories are managed based on the longest time-held disposition instruction.

> A "category" corresponds to the DB2 Records Manager File object. You must demonstrate the ability to register a single document more than once under a separate File. Each time you register the document as a record, DB2 Records Manager will create a new record entry with its own Unique Record Identifier. All record entries, however, will point back to the same document in your Host application. You must, however, record the Unique Record Identifier for each new record that you register with DB2 Records Manager. A single document in your Host Application may have more than one Unique Record Identifier.
>
> During daily processing, DB2 Records Manager may instruct the host to Delete a particular document. In addition, during disposition processing, IBM DB2 Records Manager instructs the Host to DESTROY or ACCESSION that document. The Host application must ensure that the document is NOT deleted if that document has more than one Unique Record Identifier. It must instead remove reference to that Unique Record Identifier. Only when a document is reduced to the last Unique Record Identifier can the document actually be deleted from within the Host's repository. This is also discussed in Test Section 5-1.
>
> If a multiply declared record is to be transferred (i.e. the DB2 Records Manager instructs the host application to transfer the record, but the record is declared elsewhere), then the record should be COPIED (not MOVED) from the repository and placed in the transfer directory.

Run disposition on categories... Ensure superseded records are marked as eligible for destruction, and the records in the other categories are only marked if the categories/folders are otherwise eligible. A user should have received an email notifying them that a record was superseded.

> This test relies on you having correctly installed the IRMDocumentExtension.jar logic extension. See "Logic extensions and J2EE client applications provided by IBM" on page 8

Prepare for file expunge test: Select two records from the list of records due for destruction and determine the names and locations of the files within the repository. Note the record IDs and filenames:

In order to satisfy this requirement, the host application (the one storing the records) must be able to delete the document from whatever storage device it is stored on in a way that it cannot be restored using any operating system or third party 'unerase' utilities.

TEST SECTION 9: SYSTEM MANAGEMENT

SYSTEM AUDITS

All auditing functions are carried out by DB2 Records Manager. However, because the record is actually stored in your repository, you must implement a mechanism whereby any auditable events that are executed within your host are audited. IBM DB2 Records Manager lets you record auditable events that occur in your host application(the method is called **ToolsControllerEJB.addAuditEntry**).

For details on what constitutes an auditable event, consult the *IBM DB2 Record's Administrator's Guide*.

BACKUPS AND RECOVERY

You can employ any combination of backup and recovery software and procedures to meet this requirement. Successful strategies include using the DBMS's own backup utilities in conjunction with a third party backup application.

Normally, the testers do not require a demonstration for this test if you can document your procedures and industry recognized back up and recovery software you use.

TEST SECTION 10: USABILITY EVALUATION

The tests conducted in this test section are meant to assess the usability of the product without constituting mandatory requirements.

COMPLEXITY

The DOD testers have not developed pass or fail criteria for these tests.

HELP

The DOD testers have not developed pass or fail criteria for these tests

USER INTERFACE

These features are not mandatory.

SUPPORT FOR MANAGING CLASSIFIED RECORDS

These features are supported in the DB2 Records Manager.

USER CUSTOMIZATION

Does the application allow typical users to save commonly used data in a reusable template?

> You can use the DB2 Records Manager's Defaults capability to meet this requirement. This can be performed using the DB2 Records Manager User Interface. However, when a user files a document, the host must be able to render data entry profiles based on the DB2 Records Manager profile designs and must be able to supply default values based on the DB2 Records Manager default templates.

Does the application allow typical users to save commonly used queries?

> This is supported by the DB2 Records Manager.

Does the application allow typical users to constrain their views of control tables or pick lists?

The DB2 Records Manager allows users to create user “quick-pick” lists. These were discussed in test section 5.

Does the application provide an auto-filing feature that typical users can configure?

DB2 Records Manager has an auto classify feature. For details on using the feature consult the *DB2 Records Manager Records User's Guide*. For information regarding how to use it when you render a document filing profile consult the filePlanComponent.AutoClassify method documented in *DB2 Records Manager API Reference*.

BACKWARD COMPATABILITY

You must provide a mechanism for upgrading your current software from previous DOD 5015.2 Certified versions.

Chapter 4. Summary of Requirements for Partners and What's New

This chapter is organized as follows:

- "Support for Host Content Searching"
- "Support for Host Content in the Records Manager Profile"
- "Support for DoD 5015.2 (Chap. 4) Managing Classified Records""DoD 5015.2 Requirements Summary for Partners"

Support for Host Content Searching

The IBM DB2 Records Manager has added API and **HostInterface** methods to assist Host Applications to include host metadata in Records Manager queries and to integrate host full text searches with Records Manager searches. For more information on these methods see the **HostInterface** definition in the IBM DB2 Records Manager API Reference.

Support for Host Content in the Records Manager Profile

The IBM DB2 Records Manager has added API and **HostInterface** methods to assist Host Applications to include host metadata in Records Manager File Plan Component Profiles. Host Applications will be able to display their own metadata fields directly in the Records Manager Administrator Interface. For more information on these methods see the **HostInterface** definition in the IBM DB2 Records Manager API Reference.

Support for DoD 5015.2 (Chap. 4) Managing Classified Records

The IBM DB2 Records Manager has extended the core attributes for File Plan Component to include the fields necessary to comply with DOD 5015.2-STD CHAPTER 4 requirements. Host Applications that wish to comply with this standard should be aware that they must include these new fields and apply the required business logic to Declaration data entry forms. For information on these new fields and the logic associated with them see the IBM DB2 Record's Administrator's Guide. For information on adding these fields to a host application data entry form see the IBM DB2 Records Manager Programming Guide.

DoD 5015.2 Requirements Summary for Partners

Table 2. C2.1. GENERAL REQUIREMENTS

DoD 5015.2 Requirements	Host Requirements
C2.1.1 Managing Records. RMAs shall manage records in accordance with this Standard, regardless of storage media or other characteristics (see 44 U.S.C. 3103 and 36 CFR 1222.10, references (p) and (q)).	This is a general requirement that is automatically met when the detailed requirements, described below, are fulfilled.

Table 2. C2.1. GENERAL REQUIREMENTS (continued)

DoD 5015.2 Requirements	Host Requirements
C2.1.2. Accommodating Dates and Date Logic. RMAs shall correctly accommodate and process information that contains dates in current, previous, and future centuries (see FIPS 4-2, reference (r)). The capability shall include, but not be limited to, century recognition, calculation, and logic that accommodates same century and multi-century formulas and date values, and date interface values that reflect the century. RMAs shall store years in a 4-digit format. Leap year calculations shall be accommodated (for example, 1900 is not a leap year; 2000 is a leap year).	Host application must properly handle year 2000 and leap years for all document date fields.
C2.1.3. Implementing Standard Data. RMAs shall allow for the implementation of standardized data in accordance with DoD 8320.1-M (reference (s)). When selecting commercial-off-the-shelf (COTS) products to support RMA requirements, selection criteria should include the feasibility and capability of the COTS products to implement and maintain DoD data standards. This requirement implies the capability for adding user-defined metadata fields and modifying existing field labels.	This is a general requirement that will be met automatically when the detailed requirements, described below, are met.
C2.1.4. Backward Compatibility. RMAs shall provide the capability to access information from their superseded repositories and databases. This capability shall support at least one previously verified version of backward compatibility.	If the host application provides previous versions that are also certified with this standard, the host, in conjunction with DB2 Records Manager must provide an upgrade path such that data is not lost.
C2.1.5. Accessibility. The available documentation for RMAs shall include product information that describes features that address 36 CFR parts 1194.21 and 1194.31 (references (t) and (u)). For web-based applications, 36 CFR part 1194.22 (reference (v)) shall also apply (see 29 U.S.C. 794d, reference (w)).	This is a general requirement for vendors of software to US Federal Government agencies. Software must comply with Section 508 of the Accessibility Act.

Table 3. C2.2. DETAILED REQUIREMENTS

DoD 5015.2 Requirements	Host Requirements
C2.2.1. Implementing File Plans. C2.2.1.1 RMAs shall provide the capability for only authorized individuals to create, edit, and delete file plan components and their identifiers. Each component identifier shall be linked to its associated component and to its higher-level component identifier(s) (see 44 U.S.C. 3303 and 36 CFR 1222.50, references (x) and (y)). Mandatory file plan components are shown in Table C2.T.1. Mandatory in the Structure column indicates that the field must be present and available to the user either as read/write or as read only depending upon the kind of data being stored. Mandatory in the Data Collection Required by User column indicates that RMAs shall ensure population of the associated data structure with non-null values. For fields that are not mandatory in the Data Collection column, RMAs shall behave in a predictable manner as a result of queries or other operations when the fields are not populated. The file plan components should be organized into logical sets that, when populated, will provide all the file plan references necessary to properly annotate (file) a record.	DB2 Records Manager provides full functionality for maintaining file plans. Users can use the DB2 Records Manager Web-based Administrator's User Interface to perform all aspects of File Plan management including Defining the file plan structure Defining retention schedules Assigning retention schedules to member elements of the file plan Defining the attributes that make up elements of the file plan Defining forms for data entry Defining selection lists
C2.2.1.2. RMAs shall provide the capability for authorized individuals to designate the metadata fields that are to be constrained to selection lists. RMAs shall provide the capability for authorized individuals to create and maintain selection lists (e.g., drop-down lists) for metadata items that are constrained to a pre-defined set of data.	See Requirement C2.2.1
C2.2.1.3. RMAs shall provide the capability for only authorized individuals to create, edit, and delete record folder components and their identifiers. Each component identifier shall be linked to its associated component and to its higher-level file plan component identifier(s) (see references (t) and (y)). Mandatory record folder components are shown in Table C2.T2. Mandatory in the Structure column indicates that the field shall be present and available to the user either as read/write or as read only depending upon the kind of data being stored. Mandatory in the Data Collection Required by User column indicates that RMAs shall ensure population of the associated data structure with non-null values. For fields that are not mandatory in the Data Collection column, RMAs shall behave in a predictable manner as a result of queries or other operations when the fields are not populated.	See Requirement C2.2.1
C2.2.1.4. RMAs shall ensure that identifiers (e.g., folder identifiers, record category identifiers) are unique so that ambiguous assignments, links, or associations cannot occur.	See Requirement C2.2.1

Table 3. C2.2. DETAILED REQUIREMENTS (continued)

DoD 5015.2 Requirements	**Host Requirements**
C2.2.1.5. RMAs shall provide the capability to allow only an authorized individual to define and attach user-defined business rules and/or access logic to any metadata field including user-defined fields.	See Requirement C2.2.1
C2.2.1.6. RMAs shall provide the capability to sort, view, save, and print user-selected portions of the file plan, including record folders (see reference (z)).	See Requirement C2.2.1

Table 4. C2.2.2. Scheduling Records

DoD 5015.2 Requirements	**Host Requirements**
C2.2.2. Scheduling Records. C2.2.2.1. RMAs shall provide the capability for only authorized individuals to view, create, edit, and delete disposition schedule components of record categories. C2.2.2.2. 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.	DB2 Records Manager provides a complete suite of functions for scheduling records. Records Managers can use the DB2 Records Manager Web-based user interface to perform all aspects of records scheduling including: Defining records retention schedules Defining disposition actions as a part of records retention schedules Generating schedule reports Performing schedule operations including time based schedules, event based schedules, or time-event based schedules. Performing disposition operations including Destruction, Accession and interim transfer functions Performing cutoff and close operations
C2.2.2.3. 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).	See Requirement C2.2.1

Table 4. C2.2.2. Scheduling Records (continued)

DoD 5015.2 Requirements	Host Requirements
C2.2.2.4. RMAs shall, as a minimum, be capable of scheduling and rescheduling each of the following three types of cutoff and disposition instructions (see reference (d)). 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, etc.). 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).	See Requirement C2.2.1
C2.2.2.5. RMAs shall provide the capability to automatically calculate the complete life cycle, including intermediate phases, of record folders and records not in folders (see reference (d)).	See Requirement C2.2.1
C2.2.2.6. RMAs shall provide the capability for rescheduling dispositions of record folders and/or records (those not in folders) during any phase of their life cycle if an authorized individual changes the disposition instructions. This requirement includes the capability to change the cutoff criteria of disposition instructions and to change the retention period associated with a disposition.	See Requirement C2.2.1
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).	See Requirement C2.2.1

Table 5. C2.2.3. Declaring and Filing Records

DoD 5015.2 Requirements	**Host Requirements**
C2.2.3. Declaring and Filing Records. C2.2.3.1. 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 (see reference (y)).	The requirements of the host application by the Standard are to enable the ability of a user to "declare" his/her documents as records and to associate them with one or more DB2 Records Manager record categories or folders. This constitutes the single most important point of integration between a host application, containing the records, and DB2 Records Manager, with which the records are registered. The host application must also support the ability of users to declare a single document numerous times, each time for a different record category. DB2 Records Manager treats these as separate record instances. The HOST must track how many times an individual document has been declared a record. This can be implemented using a simple reference counter in the profile of the document, or by tracking each individual record id assigned to the document by IBM DB2 Records Manager.

Table 5. C2.2.3. Declaring and Filing Records (continued)

DoD 5015.2 Requirements	Host Requirements
C2.2.3.2. Mandatory record metadata components are shown in Table C2.T3. Mandatory in the Structure column indicates that the field shall be present and available to the user either as read/write or as read only depending upon the kind of data being stored. Mandatory in the Data Collection Required column indicates that RMAs shall ensure population of the associated data structure with non-null values. For fields that are not mandatory in the Data Collection column, RMAs shall behave in a predictable manner as a result of queries or other operations when the fields are not populated.	This metadata information is Record related information and therefore must be stored as part of the record profile. The record profile can be considered to be a combination of the original document profile stored in the host, and the uniquely record related profile stored in IBM DB2 Records Manager. The complete profile should, ideally be stored in one location, either in DB2 Records Manager or in the Host. If this is not possible, then a subset of the record metadata can be stored in each application. The number of meta data columns that are shared between the host application and DB2 Records Manager should be kept to a minimum. Otherwise, the host may need to provide metadata synchronization between its own metadata and that stored in IBM DB2 Records Manager, for those shared metadata elements. When developing a strategy regarding where the record metadata is to be stored, the following factors should be considered: The ability of the host application to meet the requirements outlined in the following sections (Note: DB2 Records Manager is already able to meet those requirements.) How much metadata synchronization is acceptable between the host applications and IBM DB2 Records Manager. Any larger design or architecture considerations beyond simply "getting certified".

DoD 5015.2 Requirements	Host Requirements
C2.2.3.3. RMAs shall provide the capability for only authorized individuals to create, edit, and delete record metadata components, and their associated selection lists.	The ability to create metadata components (user defined fields) and user defined selection lists (pick lists) that populate these components is provided by IBM if it is to store the metadata defined in Table C2.T3 (as mentioned in requirement C2.2.3.2). However, depending on the host application's strategy as described in requirement C2.2.3.2, if the host application is to provide the metadata defined in Table C2.T3 then the host application must also enable the creation of user defined fields and user defined pick lists to populate those fields.
C2.2.3.4. RMAs shall provide the capability for authorized individuals to select where data collection for optional metadata fields is mandatory for a given organization.	The ability to specify which metadata components (user defined fields) are mandatory is provided by DB2 Records Manager if it is to store the metadata defined in Table C2.T3 (as mentioned in requirement C2.2.3.2) However, depending on the host application's strategy as described in requirement C2.2.3.2, if the host application is to provide the metadata defined in Table C2.T3 then the host application must also provide the ability to define which fields are mandatory.
C2.2.3.5. RMAs shall assign a unique computer-generated record identifier for each record they manage regardless of where that record is stored (see reference (z)).	DB2 Records Manager provides a unique computer generated identifier to each new record.
C2.2.3.6. RMAs shall provide the capability to create, view, save, and print the complete record metadata, or user-specified portions thereof, in user-selectable order (see reference (z)).	The ability to capability to create, view, save, and print the complete record metadata, or user-specified portions thereof is provided by DB2 Records Manager if it is to store the metadata defined in Table C2.T3 (as mentioned in requirement C2.2.3.2) However, depending on the host application's strategy as described in requirement C2.2.3.2, if the host application is to provide the metadata defined in Table C2.T3 then the host application must also provide the ability to create, view, save, and print the complete record metadata, or user-specified portions thereof.

DoD 5015.2 Requirements	**Host Requirements**
C2.2.3.7. RMAs shall provide the capability for authorized individuals to arrange record metadata components and user-defined record components on data entry screens to be used for filing.	The ability for uses to define custom data entry forms for record metadata profile is provided by DB2 Records Manager if it is to store the metadata defined in Table C2.T3 (as mentioned in requirement C2.2.3.2) However, depending on the host application's strategy as described in requirement C2.2.3.2, if the host application is to provide the metadata defined in Table C2.T3 then the host application must also provide the forms for entering the metadata. In some cases, even if DB2 Records Manager is to store the metadata, the *host may be required to show a document filing profile to the user* in order that the record metadata can be collected. DB2 Records Manager provides PROFILE DEFINITIONS that the host can use to 'render' a profile to a user.
C2.2.3.8. RMAs shall prevent subsequent changes to electronic records stored in its supported repositories. The content of the record, once filed, shall be preserved (see references (y) and (z)).	The Host application will always maintain responsibility for storage and preservation of the actual record content. The host application should never allow the record content to be altered once it has been declared a record.
C2.2.3.9. RMAs shall not permit modification of the metadata fields indicated by this Standard as not editable.	The ability for users to define custom data entry forms for record metadata profile is provided by DB2 Records Manager if it is to store the metadata defined in Table C2.T3 (as mentioned in requirement C2.2.3.2) However, depending on the host application's strategy as described in requirement C2.2.3.2, if the host application is to provide the metadata defined in Table C2.T3 then the host application must also provide the forms for entering the metadata.
C2.2.3.10. RMAs shall (for all records) capture, populate, and/or provide the user with the capability to populate the metadata elements before filing the record. RMAs shall ensure that fields designated mandatory for data collections are non-null before filing the record (see references (y) and (ah)).	See Requirement C2.2.3.7

DoD 5015.2 Requirements	**Host Requirements**
C2.2.3.11. For records that are being filed via the user interface, RMAs 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 auto-filing, RMAs shall provide the user the option of editing the record metadata prior to filing.	See Requirement C2.2.3.7
C2.2.3.12. Dates captured electronically shall be valid dates as defined in paragraph C2.1.2. Where data entry/capture errors are detected, RMAs shall prompt the user to correct the error. These prompts shall provide guidance to the user in making corrective actions; for example, "Date format incorrect - use MM/DD/YYYY."	Host application must properly handle dates for all document date fields.
C2.2.3.13. RMAs shall restrict the capability to only authorized individuals to define and add user-defined metadata fields (e.g., project number, budget line) for site-specific requirements (see reference (ah)).	The DB2 Records Manager provides the ability to add user-defined metadata fields.
C2.2.3.14. RMAs shall provide the capability to view, save, or print the metadata associated with a specified record or set of records, or user-specified portions thereof, in user-selectable order.	See Requirement C2.2.3.6
C2.2.3.15. RMAs shall provide the capability for only authorized individuals to limit the record folders and record categories presented to a user or workgroup. Based on these limits, RMAs shall present to users only those record categories or folders available to the user or workgroup for filing.	*Security (including specifying into which folders or record categories any particular user can file) is performed by IBM DB2 Records Manager*
C2.2.3.16. RMAs shall provide the capability for only authorized individuals to change a record folder or record category associated with a record.	Once a record has been declared, records managers assign it to a different record category or folder. This is accomplished using the IBM DB2 Records Manager's own records user interface. Alternatively the host application can expose this feature to its users by employing the IBM DB2 Records Manager API.
C2.2.3.17. RMAs shall provide a capability for referencing or linking and associating supporting and related records and related information, such as notes, marginalia, attachments, and electronic mail-return receipts, etc., to a specified record. RMAs shall allow only authorized individuals to change or delete links and associations (see reference (z)).	Part of the act of declaring a document as a record may also be to 'link' it to related records. This feature is provided using the IBM DB2 Records Manager's records administrator interface. For normal users who may not have access to the IBM's Web-based records administrator's interface, this feature can be implement by the host application, using the IBM DB2 Records Manager API.
C2.2.3.18. RMAs shall provide the capability to link original superseded records to their successor records.	See Requirement C2.2.3.17

DoD 5015.2 Requirements	Host Requirements
C2.2.3.19. RMAs shall provide the capability to support multiple renditions of a record. These shall be associated and linked.	For the purposes of certification IBM interprets 'renditions' to mean alternative digital formats of the same record. These can be a TIFF of an original scanned document, and the accompanying OCR text. Because all record content is stored in the originating host application, the host must be able to store alternative digital formats. These can be considered different DOCUMENTS by the host so long as they only have ONE RECORD entry in the IBM DB2 Records Manager DB.
C2.2.3.20. RMAs shall provide the capability to increment versions of records when filing. RMAs shall associate and link the versions.	The host application must be able to support 'document versions' such that a new version of a document can be created from an existing document. These two versions can be declared separately as records in IBM DB2 Records Manager. DB2 Records Manager supports the ability to LINK different records together. This can be done when the new version of the document is declared a record with IBM DB2 Records Manager. This must be done explicitly using the DB2 Records Manager API by the host application.
C2.2.3.21. RMAs shall link the record metadata to the record so that it can be accessed for display, export, etc. (see 36 CFR 1234.32, reference (ai)).	DB2 Records Manager contains a field in the record profile named **XtRecID** (External Record ID). The host application, when declaring a document as a record, must supply a string for this field that globally uniquely identifies that document to IBM DB2 Records Manager.
C2.2.3.22. RMAs shall provide the capability for only authorized individuals to modify the metadata of stored records. However, RMAs shall not allow the editing of metadata fields that have been specifically identified in this Standard as not editable.	See Requirement C2.2.3.7
C2.2.3.23. RMAs shall enforce data integrity, referential integrity, and relational integrity. C2.2.3.24. RMAs shall provide the capability to automatically synchronize multiple databases and repositories.	

DoD 5015.2 Requirements	Host Requirements
C2.2.3.25. RMAs shall provide the capability for users to create and maintain shortened "quick–pick" lists from the authorized lists.	A "quick-pick" list is exclusive to a single user and is a subset of an authorized pick list. DB2 Records Manager supports quick-pick lists. If the host renders a document filing profile to the user (see Requirement C2.2.3.7), the host must implement the ability to render quick-pick lists in the filing form.
C2.2.3.26. RMAs shall provide the capability for users to create and maintain templates that automatically populate commonly used data into record metadata fields.	DB2 Records Manager supports the ability to create 'defaults templates'. These can be used if DB2 Records Manager web-based user interface is also being used to provide data entry forms (see Requirement C2.2.3.7). Otherwise, if the host application is rendering the profile, the host application must provide a method to store defaults templates and apply those defaults when rendering the data entry form.
C2.2.4. Filing Electronic Mail Messages (E-mail).	Collecting emails and storing them in the RMA's repository is a mandatory feature for any RMA that meets the DOD 5015.2 standard.
C2.2.4.1. RMAs shall treat e-mail messages the same as any other record, and these shall be subject to all requirements of this Standard (see 32 CFR 1222.32 and 36 CFR 1234.24, references (aj) and (ak)).	Email is to be stored like any other document in the host application's document repository.
C2.2.4.2. RMAs shall capture and automatically store the transmission and receipt data identified in Table C2.T4 if available from the e-mail system, as part of the record metadata when an e-mail message is filed as a record (see reference (ak)). RMAs shall provide the capability for editing Subject or Title, Author or Originator, Addressee(s), and the Other Addressee(s) metadata fields prior to filing. All other fields shall not be editable.	DB2 Records Manager has a Microsoft Outlook Plug-in utility that enables host applications to collect the appropriate metadata from the email metadata and store them as record metadata. This plug-in can be used only if DB2 Records Manager is to be used to store all the mandatory record meta data listed in Table C2.T3 (as mentioned in requirement C2.2.3.2) If your integration strategy is such that the host application will store the record metadata or if you will be using an email package other than MS Outlook, you must provide your own plug-in. For details consult the email integration section of this Guide.

DoD 5015.2 Requirements	**Host Requirements**
C2.2.4.3. RMAs shall provide the user the option of filing e-mail and all its attachment(s) as a single record, or filing selected e-mail item(s) as individual record(s), or to do both. When the attachment(s) is (are) filed as individual record(s), the user shall be provided the capability to enter the metadata required in table C2.T3. (see reference (ak)).	The host application shall be responsible for implementing functionality such that emails and their associated attachments can be stored as a single document, as separate documents, or both. This is a straightforward task if you are integrating with MS Outlook.
C2.2.5. Storing Records.	
C2.2.5.1. RMAs shall provide at least one portal that provides access to all associated repositories and databases storing electronic records and their metadata.	Storing records is the responsibility of the host application.
C2.2.5.2. The RMAs shall prevent unauthorized access to the repository(ies) (see 36 CFR 1222.50 and 44 U.S.C. 3105, references (y) and (al)).	Managing access to the repository is the responsibility of the host application. The DB2 Records Manager supplies methods to help synchronize record permissions with their corresponding content.
C2.2.5.3. 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 (see references (y), (z), and (ah)).	The responsibility of the host application.
C2.2.5.4. RMAs shall allow only authorized individuals to move or delete records from the repository (see 36 CFR 1222.50 and 36 CFR 1234.28, references (y) and (am)).	The responsibility of the host application.
C2.2.6. Retention and Vital Records Management.	
C2.2.6.1. Screening Records.	Screening of records is exclusively the responsibility of IBM DB2 Records Manager. These functions can all be accomplished using the DB2 Records Manager Web-based user interface.

DoD 5015.2 Requirements	Host Requirements
C2.2.6.1.1. 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	
C2.2.6.1.2. RMAs shall provide for sorting, viewing, saving, and printing life cycle information, eligibility dates, and events of user-selected record folders and records.	
C2.2.6.1.3. RMAs shall allow the user to select and order the columns presented in the screening result list(s).	
C2.2.6.1.4. 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.	
C2.2.6.1.5. RMAs shall provide for sorting, viewing, saving, and printing lists and partial lists of record folders and/or records that have no assigned disposition.	
C2.2.6.2. Closing Record Folders.	Closing record folders is exclusively the responsibility of IBM DB2 Records Manager. These functions can all be accomplished using the IBM DB2 Records Manager Web-based user interface.
C2.2.6.2.1. RMAs shall provide a capability for authorized individuals to close record folders to further filing after the specified event occurs.	
C2.2.6.2.2. 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.	
C2.2.6.3. Cutting Off Record Folders.	Cutting Off Record Folders is exclusively the responsibility of IBM DB2 Records Manager. These functions can all be accomplished using the IBM DB2 Records Manager Web-based user interface.

DoD 5015.2 Requirements	Host Requirements
C2.2.6.3.1. 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 (see reference (z)).	
C2.2.6.3.2. RMAs shall provide the capability to only authorized individuals to add records or make other alterations to record folders that have been cut off.	
C2.2.6.4. Freezing/Unfreezing Records.	Freezing/Unfreezing of records is exclusively the responsibility of IBM DB2 Records Manager. These functions can all be accomplished using the IBM DB2 Records Manager Web-based user interface.
C2.2.6.4.1. 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 (see 44 U.S.C. 2909 and 36 CFR 1228.54, references (an) and (ao)).	
C2.2.6.4.2. RMAs shall provide a field for authorized individuals to enter the reason for freezing a record or record folder.	
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.	
C2.2.6.4.4. RMAs shall allow authorized individuals to search, update, and view the reason for freezing a record or record folder.	

DoD 5015.2 Requirements	Host Requirements
C2.2.6.5. Transferring Records.	Transferring records entails sending them to be stored at an outside authority or application. The DoD 5015.2 test procedures define two types of transfers: Interim Transfers and Final Accessions. Interim Transfers are transfers whereby the record is moved to an off-site storage facility but remains the responsibility of the organization operating the RMA. Final accessions are forms of disposition whereby the record is given to an outside authority (normally the National Archives) and is no longer under the domain of the RMA. In both cases the DoD 5015.2 test procedures employ a simple concept whereby the records are extracted from the repository and copied to a staging area from where they can be written to CD, tape or some other portable media. This staging area is to be considered an extension of the repository with all the protection that entails. This is the responsibility of the hosting application.
C2.2.6.5.1. RMAs shall identify and present those record folders and records eligible for interim transfer and/or accession.	DB2 Records Manager is designed to perform all life cycle calculations. This includes determining when a record is eligible to be transferred out of the RMA. DB2 Records Manager provides a complete user interface that provides users with lists of records eligible for transfer.

DoD 5015.2 Requirements	Host Requirements
C2.2.6.5.2. 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. For permanent records to be accessioned to the National Archives, the accessioning file(s) be made to conform to one of the formats and media specified in 36 CFR 1228.270. **Note:** If accessioning records and metadata to NARA in a format and media specified in 36 CFR 1228.270 causes a violation of the records' authenticity and/or integrity, the organization should contact NARA for guidance, see C2.2.10.5.	This is a joint responsibility between DB2 Records Manager and the Host Application. The host application must implement the **HostInterface** interface defined in the com.ibm.gre.engine.recordhost package. This interface contains the **phaseTransition** method that the host must implement. IBM DB2 Records Manager, will perform all necessary life cycle calculations and enable the user to pick the records to be transferred. For those records, DB2 Records Manager will invoke the Host's implementation of the **HostInterface**. The host must do two things: the host must extract the record from its repository and placed it in a predefined location It must return any pertinent metadata to DB2 Records Manager for inclusion in the transfer metadata file.
C2.2.6.5.3. 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. For permanent records to be accessioned to the National Archives, the metadata shall be made to conform to one of the formats and media specified in 36 CFR 1228.270.	Normally, non-electronic records are profiled exclusively using IBM DB2 Records Manager. In this case, the host application is not responsible for any aspects of this requirement. If the host chooses to maintain profiles (for example, meta data) for non-electronic records such as paper documents, maps, and books, then it will be responsible to store and extract the meta data in a manner similar to that described in C2.2.6.5.2.
C2.2.6.5.4. 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 (see references (al) and (ao)). RMAs shall provide the capability to allow the organization to retain the metadata for records that were transferred or accessioned.	IBM's recommendations for this requirement is to Move all records and their metadata (in the form of XML files) to a staging area from which they can be written to CD, Tape or other portable media. This staging area is to be considered an extension of the repository and must be afforded the same protections as the repository. Once confirmation of receipt of the transferred records is received, this staging area can then be deleted.

DoD 5015.2 Requirements	Host Requirements
C2.2.6.5.5. RMAs shall provide documentation of transfer activities. This documentation shall be stored as records.	DB2 Records Manager generates a log file containing a list of all file plan components transferred, accessioned, destroyed, etc. This log file can be refilled as a record.
C2.2.6.6. Destroying Records.	
C2.2.6.6.1. 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.	All calculations and presentations of lists of records eligible for destruction is the responsibility of IBM DB2 Records Manager. The host, however, must implement at the **HostInterface** found in the com.ibm.gro.engine.recordhost package. For each record selected for destruction IBM DB2 Records Manager will invoke the host's implementation of the **HostInterface** and call the destroy method. The host's implementation of the destroy method will be to ensure that if the document is registered as a record numerous times, to only remove the reference to the record ID being deleted, and not to actually delete (destroy) the record. If however the document is only registered once, or it is no longer referenced by any additional record ids, then the document must be destroyed.
C2.2.6.6.2. 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.	This UI feature is implemented in IBM DB2 Records Manager.
C2.2.6.6.3. RMAs shall delete electronic records approved for destruction in a manner such that the records cannot be physically reconstructed.	Destroying records entails deleting them from their electronic storage media in such a way that they cannot be restored or recovered by any utility commonly available.
C2.2.6.6.4. RMAs shall provide an option allowing the organization to select whether to retain or delete the metadata of destroyed records	This UI feature is implemented in IBM DB2 Records Manager.
C2.2.6.6.5. RMAs shall restrict the records destruction commands to authorized individuals.	The IBM DB2 Records Manager restricts the **deleteFilePlanComponent** method to authorized users.
C2.2.6.6.6. RMAs shall provide documentation of destruction activities. This documentation shall be stored as records.	IBM DB2 Records Manager generates a log file containing a list of all file plan components transferred, accessioned, destroyed, etc. This log file can be refilled as a record.

DoD 5015.2 Requirements	Host Requirements
C2.2.6.7. Cycling Vital Records.	Cycling Vital records can only be performed using IBM DB2 Records Manager.
C2.2.6.7.1. RMAs shall provide the capability for authorized users to enter the Vital Records Review and Update Cycle Period when creating or updating the file plan.	
C2.2.6.7.2. RMAs shall provide the capability to enter the date when the records associated with a vital records folder have been reviewed and updated.	
C2.2.6.7.3. RMAs shall provide a means for identifying and aggregating vital records due for cycling.	
C2.2.6.7.4. RMAs shall provide a means for identifying and aggregating vital records by previous cycle dates.	
C2.2.6.8. Searching for and Retrieving Records.	Searching for and Retrieving records is fully supported using the IBM DB2 Records Manager reporting user interface. If the IBM DB2 Records Manager is also responsible for maintaining all record metadata, then DB2 Records Manager searching facility can be used. However, if the host application is storing some or all of the records metadata, the requirements listed under C2.2.6.8.1 to C2.2.6.8.9 must also be supported by the host application. Because records continue to be stored in the originating host application, retrieval of records will be a joint responsibility. Searching is carried out using the DB2 Records Manager. The host, therefore, must provide a mechanism for a user, logged into the DB2 Records Manager, to be able to retrieve a document from the host's repository. See section 6 of this document for a way to integrate DB2 Records Manager's search capability with the retrieval of a document from the host.
C2.2.6.8.1. RMAs shall allow users to browse the records stored in the file plan based on their user access permissions.	
C2.2.6.8.2. RMAs shall allow searches using any combination of the record and/or folder metadata elements.	
C2.2.6.8.3. RMAs shall allow the user to specify partial matches and shall allow designation of "wild card" fields or characters.	

DoD 5015.2 Requirements	**Host Requirements**
C2.2.6.8.4. RMAs shall allow searches using Boolean logic terms: "and," "and not," "or," "greater than" (>), "less than" (<), "equal to" (=), and "not equal to" (<>), and provide a mechanism to control the order of precedence.	
C2.2.6.8.5. 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.	
C2.2.6.8.6. RMAs shall allow users the ability to search for null or undefined values.	
C2.2.6.8.7. 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 for filing.	
C2.2.6.8.8. 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.	
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.	
C2.2.6.8.10. RMAs shall allow users to select any number of records, and their metadata, for retrieval from the search results list.	
C2.2.6.8.11. RMAs shall allow the user to abort a search.	
C2.2.7. Access Control. Table C2.T5. summarizes requirements that refer to "authorized individuals" and offers additional information regarding example user-type roles and responsibilities. Typically, Application Administrators are responsible for setting up the RMA infrastructure. Records Managers are responsible for records management administration. Privileged Users are those who are given special permissions to perform functions beyond those of typical users. RMAs shall provide the capability to allow organizations to define roles and responsibilities to fit their records management operating procedures.	Maintenance of Security, as it is defined for the Standard, pertains to records management functions and is therefore the responsibility of IBM DB2 Records Manager.

DoD 5015.2 Requirements	Host Requirements
C2.2.7.1. The RMA, in conjunction with its operating environment, shall use authentication measures that allow only authorized persons access to the RMA. At a minimum, the RMA will implement authentication measures that require: C2.2.7.1.1. Userid. C2.2.7.1.2. Password. RMAs shall provide the capability for authorized users to define the minimum length of the Password field. C2.2.7.1.3. Alternative methods, such as Biometrics, Common Access Cards (CAC), or Public Key Infrastructure (PKI), in lieu of or in conjunction with the above, are acceptable. If used in lieu of, the alternative must provide at least as much security.	This is a joint responsibility. See Host Authentication for details on how the host application and DB2 Records Manager can jointly manage users and groups. The host application must ensure that authorized users are able to specify minimum password and userid lengths.
C2.2.7.2. RMAs shall provide the capability for only individuals with Application Administrator access to authorize access capabilities to any combination of the items identified in Table C2.T5. to individuals and to groups.	This is the responsibility of IBM DB2 Records Manager.
C2.2.7.3. 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.	This is the responsibility of IBM DB2 Records Manager.
C2.2.7.4. 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.	This is a host requirement as well as an DB2 Records Manager requirement.
C2.2.7.5. RMAs shall support simultaneous multiple-user access to all components of the RMA, the metadata, and the records.	This is the responsibility of IBM DB2 Records Manager.
C2.2.8. System Audits.	
C2.2.8.1. 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. These actions include retrieving, creating, deleting, searching, and editing actions (see references (c) and (ar)). Logging of searching and retrieving actions are not required for User Accounts and User Groups.	This is a joint responsibility. The host application must inform DB2 Records Manager of any activities such as, activities relating to the viewing, deleting, editing or copying of a record. Or changing user accounts.

DoD 5015.2 Requirements	Host Requirements
C2.2.8.2. The RMA shall provide a capability whereby an authorized individual can determine which of the specified actions listed in C2.2.8.1. are audited.	This is the responsibility of IBM DB2 Records Manager.
C2.2.8.3. 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. These are the specified actions listed in subparagraph C2.2.8.1 (see references (c) and (z)). 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.	This is the responsibility of IBM DB2 Records Manager.
C2.2.8.4. RMAs shall provide the capability to file the audit data as a record.	DB2 Records Manager provides the ability to export audit reports as XML files. These files can then be stored in the HOST document repository and declared as records.
C2.2.8.5. RMAs shall allow only authorized individuals to backup and remove audit files from the system.	This is the responsibility of IBM DB2 Records Manager.
C2.2.9. System Management Requirements. The following functions are typically provided by the operating system or by a database management system. These functions are also considered requirements to ensure the integrity and protection of organizational records. They shall be implemented as part of the overall records management system even though they may be performed externally to an RMA.	This is a joint responsibility between the host application and IBM DB2 Records Manager.
C2.2.9.1. Backup of Stored Records. The RMA system shall provide the capability to automatically create backup or redundant copies of the records.	This is a joint responsibility between the host application and IBM DB2 Records Manager.
C2.2.9.2. Storage of Backup Copies. 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 destruction.	This is a joint responsibility between the host application and IBM DB2 Records Manager.
C2.2.9.3. Recovery/Rollback Capability. 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 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	This is a joint responsibility between the host application and IBM DB2 Records Manager.

DoD 5015.2 Requirements	Host Requirements
C2.2.9.4. Rebuild Capability. The system shall provide the capability to rebuild from any backup copy, using the backup copy and all subsequent system audit trails.	This is a joint responsibility between the host application and IBM DB2 Records Manager.
C2.2.9.5. Storage Availability and Monitoring. 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.	This is a joint responsibility between the host application and IBM DB2 Records Manager.
C2.2.9.6. Safeguarding. The RMA, in conjunction with its operating environment, shall have the capability to activate a keyboard lockout feature and a screen-blanking feature.	This is normally handled within the operating system.

Table 6. MANAGEMENT OF CLASSIFIED RECORDS

DoD 5015.2 Chap. 4 Requirements	Host Requirements
C4.1. REQUIREMENTS FOR RMAS SUPPORTING MANAGEMENT OF CLASSIFIED RECORDS The following requirements address the management of classified records. As such, these requirements are only mandatory for those RMAs that manage classified records. These requirements are in addition to those requirements outlined in Chapters 2 and 3. In this chapter, the word "shall" identifies mandatory system standards for vendors who support the management of classified records. The word "should" identifies design objectives that are desirable but not mandatory for supporting classified records management. Additionally, requirements for safeguarding and providing security for classified records are not in the scope of this document, since they are provided in other more applicable directives and regulations.	The IBM DB2 Records Manager fully supports these requirements. Host applications that wish to render their own declaration forms will be responsible for adhering to the User Interface Requirements specified below.
C4.1.1. Mandatory Metadata Fields for Classified Records. RMAs shall provide a capability by which a user can add metadata that describes a classified record. These metadata elements are shown in Table C4.T1. Mandatory in the Structure column indicates that the field shall be present and available to the user either as read/write or as read only depending upon the kind of data being stored. Mandatory in the Data Collection Required by User column indicates that RMAs shall ensure population of the associated data structure with non-null values. For fields that are not mandatory in the Data Collection column, RMAs shall behave in a predictable manner as a result of queries or other operations when the fields are not populated.	The IBM DB2 Records Manager supports all metadata that describes a classified record.
C4.1.2. Initial and Current Classification. RMAs shall populate the Current Classification field with the Initial Classification data when the Initial Classification is first entered.	Host applications that wish to render their own declaration forms are responsible for this requirement.

Table 6. MANAGEMENT OF CLASSIFIED RECORDS (continued)

DoD 5015.2 Chap. 4 Requirements	Host Requirements
C4.1.3. Current Classification. RMAs shall provide a capability by which a user can edit the Current Classification field prior to filing.	Host applications that wish to render their own declaration forms are responsible for this requirement.
C4.1.4. Originally Classified Records. RMAs shall require that when the “Derived From” field is not completed, the “Classified By” and “Reason(s) for Classification” fields must be completed.	The IBM DB2 Records Manager will validate this condition.
C4.1.5. Derivatively Classified Records. When the “Derived From” field is populated, RMAs shall provide the option of capturing multiple “Reason(s) for Classification” and “Classified By” fields.	Host applications that wish to render their own declaration forms are responsible for this requirement.
C4.1.6. Derivative Sources. When the classified information is derived from multiple sources, RMAs shall provide the capability to enter multiple sources.	Host applications that wish to render their own declaration forms are responsible for this requirement.
C4.1.7. Declassify On Event. When “Event” is selected in the “Declassify On” field, the RMA shall prompt the user to enter text that describes the de-classification event.	Host applications that wish to render their own declaration forms are responsible for this requirement.
C4.1.8. Declassify On Time Frame. When a date is inserted in the “Declassify On” field, RMAs shall verify that the date is no more than the mandated period of time from the Publication Date. If that time frame is exceeded, an alert shall be presented to the user. This mandatory period is currently 10 years.	The IBM DB2 Records Manager validates this condition.
C4.1.9. Maintaining the Declassify On Time Frame. RMAs shall provide the capability for authorized individuals to establish and maintain the period of time used to verify the “Declassify On” field, both to make the retention period more restrictive or to accommodate changes to the mandatory retention period.	The IBM DB2 Records Manager supports this requirement from within the Administrator web application.
C4.1.10. Classification Guides. RMAs shall provide a capability that allows an authorized individual to establish an automatically triggered classification mechanism. When a designated classification guide indicator is entered in the “Derived From” field, the following fields shall be automatically populated: C4.1.10.1. Reason(s) for Classification. C4.1.10.2. Initial Classification. C4.1.10.3. Declassify On.	Host applications that wish to render their own declaration forms are responsible for this requirement.
C4.1.11. Confirming Accuracy Prior to Filing. RMAs shall provide the capability to confirm the accuracy of all user editable metadata items prior to filing.	Host applications that wish to render their own declaration forms are responsible for this requirement.
C4.1.12. Editing Records. RMAs shall allow only authorized individuals to edit metadata items after a record has been filed.	The IBM DB2 Records Manager supports this requirement.

Table 6. MANAGEMENT OF CLASSIFIED RECORDS (continued)

DoD 5015.2 Chap. 4 Requirements	Host Requirements
C4.1.13. Restricted Data and Formerly Restricted Data. The following metadata items are not applicable for records containing Restricted Data or Formerly Restricted Data [Supplemental Marking(s)] and shall be disabled. C4.1.13.1. Downgrade On. C4.1.13.2. Declassify On.	Host applications that wish to render their own declaration forms are responsible for this requirement.
C4.1.14. Current Classification. When the entry in the “Current Classification” field is changed, RMAs shall ensure that “Upgraded On”, “Downgraded On”, or “Declassified On” field, whichever is appropriate, is populated with an appropriate date field.	Host applications that wish to render their own declaration forms are responsible for this requirement.
C4.1.15. Exemption Categories. RMAs shall provide the capability for an authorized individual to enter or update exemption category(ies) in the “Declassify On” field.	Host applications that wish to render their own declaration forms are responsible for this requirement.
C4.1.16. Record History Audit. The RMA shall capture and link an audit history of each record by capturing the replaced metadata value and the person who entered that value, and appending them to a record audit history file. The metadata fields to be captured shall be authorized individual selectable.	The IBM DB2 Records Manager supports this requirement.
C4.1.17. Using the Record History Audit. The RMA shall provide the capability to view, copy, save, and print the record history file based on user permissions; shall not allow the editing of the record history file; and shall provide the capability for only authorized individuals to delete the record history file	The IBM DB2 Records Manager supports this requirement.
C4.1.18. Marking Printouts and Displays. Current classification, reasons for classification, and downgrading instructions shall be required metadata items for displays, printouts, reports, queries, review lists, etc. The highest classification level shall be displayed when aggregate results are displayed.	The IBM DB2 Records Manager reporting UI supports this.
C4.1.19. The RMA, in conjunction with its operating environment, shall ensure that if there is a conflict between the individual’s access criteria and the access criteria of the group(s) assigned, the individual’s access criteria shall take precedence.	The IBM DB2 Records Manager supports this requirement.
C4.1.20. The RMA shall provide a capability whereby authorized individuals restrict access to records and their metadata based on access criteria. In addition to baseline access restriction capabilities, these additional criteria include. C4.1.20.1. Current Classification C4.1.20.2. Supplemental Marking List C4.1.20.3. Metadata Elements identified by the organization to be used for access control.	The IBM DB2 Records Manager supports this requirement.

Table 6. MANAGEMENT OF CLASSIFIED RECORDS (continued)

DoD 5015.2 Chap. 4 Requirements	**Host Requirements**
C4.1.21. Access Control. Table C4.T2. summarizes requirements that refer to “authorized individuals” and offers additional information regarding user-type responsibilities. In general, Application Administrators are responsible for setting up the RMA infrastructure. Records Managers are responsible for records management administration. Privileged Users are those who are given special permissions to perform functions beyond those of typical users.	The IBM DB2 Records Manager supports this requirement.

Chapter 5. IBM email Module for Microsoft Outlook

IBM DB2 Records Manager includes a working application for capturing Microsoft Outlook 2000 email according to DoD 5015.2 requirements. This application consists of an ActiveX DLL that provides the forms based user interface and a Microsoft Outlook 2000 macro that can be customized to suit your requirements.

IBM provides this application to assist partners in satisfying the DoD 5015.2 email specific requirements. One of the requirements mandated by the DoD 5015.2 standard is that the application be able to capture email records in a very specific manner and format. The IBM Outlook e-mail module provides all of the necessary user interface functionality required.

The IBM Outlook e-mail Module performs the following tasks:

1. Provides a DoD 5015.2 compliant email capture application
2. Connects the application into the email **send** event so that the application is automatically invoked whenever an email is sent by default.
3. Provides for manual invocation of the application through the "DeclareMailItem" subroutine in the *IRMMacros.bas* macro file.
4. When the *DeclareMailItem* macro is called, a login screen displays. The user's login information is cached and they will not have to login again. This login form accepts login credentials for DB2 Records Manager.
5. Renders a forms-based user interface compliant with the DoD 5015.2 requirements. All of the user's configuration settings (profiles, defaults, pick-lists, attributes) are read and applied appropriately to the displayed form.
6. Provides DoD compliant classification assistance (including auto-classify)
7. Provides data verification of input meta data
8. Creates a new email object in the file plan consisting of the input meta data

The Outlook email module included with the Toolkit is not complete. A couple of steps must be provided by the host application before the email module is fully operational. The host application must provide the following:

1. Store the email message in the host repository and retrieve the document id.
2. Update the email record XML with the **XtRecId** (host document id) and the **RecHsId** (the host ID)
3. Create the email record in DB2 Records Manager and retrieve the internal DB2 Records Manager file plan component ID.
4. Update the host document with the DB2 Records Manager file plan component ID. This will effectively cross reference the host document to the DB2 Records Manager record.

   Notes:
   Note

   a. You should also denote this document is now a record through a document attribute
   b. You must be able to record MULTIPLE record ids with each document to cover the situation that a single record may be registered multiple times into different file plan components (for example, Files).

      Now the Outlook e-Mail module should be operational. The reason that you must provide the previous four steps is that they are unique for each partner's host application. The steps are clearly documented in the IRMMacros.bas file with comment lines

If any of the previous steps results in an error, then it is your responsibility to "rollback" the transaction. This would mean deleting the document from the host repository and deleting the email record from DB2 Records Manager if required.

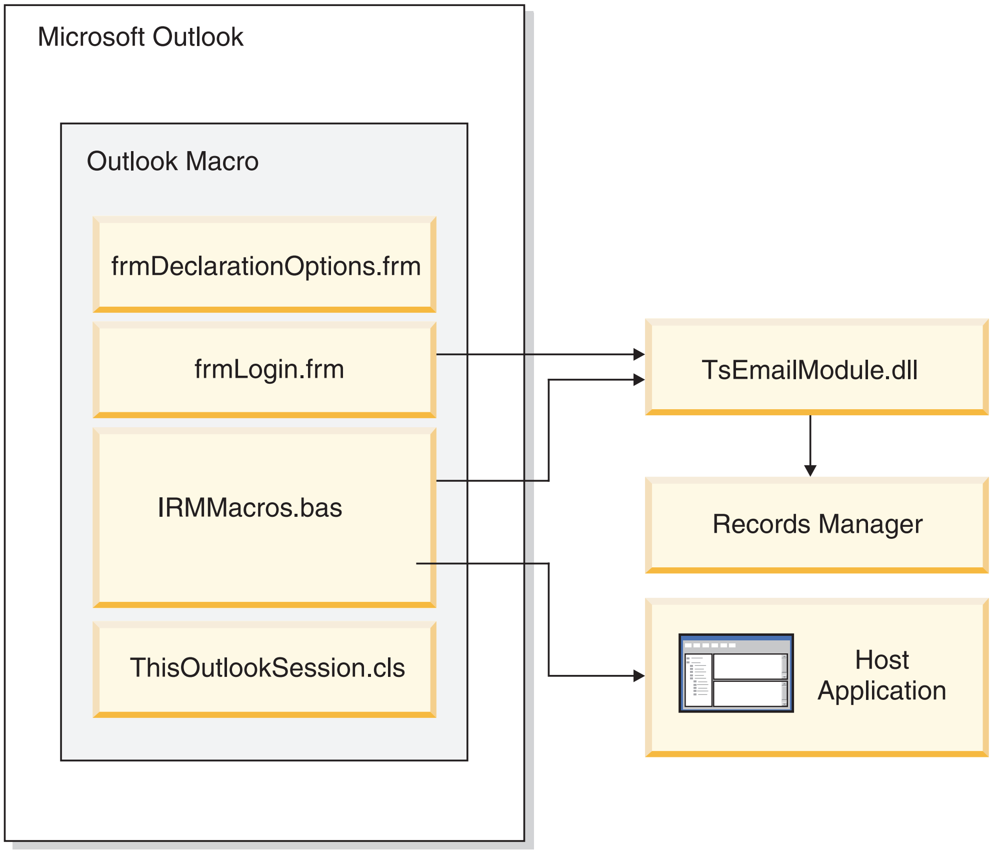
Email Module architecture

The next diagram illustrates how the IBM Outlook email module components interact. The main IBM outlook macro is loaded manually into Microsoft Outlook. It consists of:

FrmDeclarationOptions.frm	This form provides a selection form for how the email and it's attachments are to be stored.
FrmLogin.frm	This form provides a login form
IBMMacro.bas	This module provides the logic to load the input form and process the results. This is the module that you must modify to provide integration with the host repository.
ThisOutlookSession.cls	This class provides the **ItemSent** event handler which allows the macro to trap send email events.

The *IRMEmailModule.dll* is an ActiveX DLL that provides the user interface that is compliant with the DoD 5015.2 email requirements. This DLL communicates with DB2 Records Manager to render the proper form for the logged in user, validate the input data, and pass the recorded meta data to the macro for storage in DB2 Records Manager.

Note: Within *IRMMacro.bas*, you must provide code as described above to store the email message and its attachments in the host repository and synchronize the host document with the DB2 Records Manager record.



The IBM Outlook e-Mail module uses a file called "fieldmappings.xml" if it exists in the same directory as IRMEmailModule.dll. This XML file can be used to specify which outlook email message fields you want to map into which DB2 Records Manager custom attributes if you wish to override the default mappings (as specified in the "DoD 5015.2 walkthrough")

```
<FieldMapping From="Ts_From" Addressees="Ts_Addressees"
 OtherRecipients="Ts_OtherRecipients" Subject="FlPlnCmpntTtl"
 SentDate="Ts_EmailSentDate" ReceivedDate="Ts_EmailReceivedDate"
/>
```

You can edit the file and specify the name of the DB2 Records Manager custom attribute you wish to override.

From the above XML file, the attribute name is the field name in Outlook and the value is the custom attribute column name in email component definition.

Note: The attribute Subject is mapped to the value **FlPlnCmpntTtl** that is a core attribute of the file plan component definition for email component definition.

Email Module configuration

Before you can use the email macro you must configure DB2 Records Manager to support your email objects. Specifically, you must create the following items in DB2 Records Manager. You can do this using the Web client or the API.

Views

Create a view of type Link and call it Cross-Reference, take note of the view ID this will be used later in macro customization. Add a relationship definition for the view. Call this relationship definition “Cross Reference”.

Name	Type	Comments
DOD 5015.2	Hierarchical	Create this view if it does not exist.
Cross-Reference	Link	New link view

Component Definitions

Create two component definitions of type record with primary view of DOD 5015.2 and name one **email**, and the other **document** and **version**.

Take note of the component definition ID of each component created, this will be needed later in the macro customization.

Name	Type	Comments
Email	Record	In DOD 5015.2 view
Document	Record	In DOD 5015.2 view

Relationship definitions in the DoD 5015.2 view

In order to upload attachments, you need to create a relationship between Document and Version. IBM DB2 Records Manager stores the attachment under **Version** for the related document.

Relationship definitions in Cross-Reference view

Create two relationship definitions in the Cross-Reference view as follows:

From	To
Email	Document
Document	Document

Custom Attributes

Create additional custom attributes in both email and document component definitions as required for DOD 5015.2 compliancy.

Name	Type	Comments
From	String	
Addressees	String	
OtherRecipients	String	
EmailReceivedDate	String Or Date	See readme notes YYYY-MM-DDTHH:mm:ssZ

After you complete these steps, you can configure the "declarations" section of the *IRMMacros.bas* file. Replace the default ids with the actual ids of the items you have created previously and update the name and port number of the **IRMWebServices** URL.

Public Const lEmailID As Variant = 41

Public Const lAttachmentID As Variant = 42

Public Const lCrossReferenceViewID As Variant = 41

Public Const IRM_EMAIL = ″IRM 4.1 Email″

Public Const strServerURL As String = ″http://localhost:9080/IRMWebServices/services/″

Email Module installation

You must manually install the IBM Outlook e-Mail Macro into Outlook 2000. The installation process does not do this automatically. Please perform the following steps:

1. Start Microsoft Outlook.
2. Open **Visual Basic Editor** by selecting **Tools > Macros > Visual Basic Editor** or by pressing **ALT + F11**.
3. Right Click on **Project1** project and select **Import File** menu.
4. Navigate to the directory where IBM DB2 Records Manager is installed.
5. Change to directory *Email Module\Outlook Macros*.
6. Import the following four files:
   - fmDeclarationOptions.fm
   - fmDeclarationOptions.frx
   - IRMMacros.bas
   - ThisOutlookSession.cls
7. Expand **Class Modules** in the **Project Explorer**.
8. Double-click **ThisOutlookSession1** class.
9. Select all source code in that class and copy it to the clipboard.
10. Expand **Microsoft Outlook Objects** in the **Project Explorer**.
11. Double-click **ThisOutlookSession**.
12. Paste source code.
13. Select **Tools > References** and configure project references.

    Note: IRMProxies.tlb and IRMEmailModule.dll are required. Please ensure that these are checked in the **References** dialog box. The .NET Framework must be installed.
14. Change global constants **lEmailID**, **lAttachmentID** and **lCrossReferenceViewID** to reflect your file plan ids for email file plan component definition, attachment file plan component definition and cross reference view id.
15. Save your Outlook project and close **Visual Basic Editor**.
16. In Outlook, right click on the toolbar and select **Customize**.
17. Select the **Toolbars** tab and click **New**.

18. Pick a name for a new button and click “OK”.
19. Select the **Commands** tab.
20. In the **Categories** list, select **Macros**.
21. A list of available Commands appears on the right.
22. Select them one by one and drag and drop each of them on the newly created toolbar.
23. The name of command on the toolbar can be changed by right clicking on the command and changing the name.
24. By default the main declaration function in the macro is commented out (disabled).
25. To modify the behavior to suite your application open V**isual Basic Editor**.
26. In **Project Explorer**, expand **Modules** and double click the **IRMMacros** module.

Macro Security Issues

Note: If macro security is turned on with a security level of high, the macros will not work. Because this is only a test environment, we will change the security setting to Medium. This can be done from Tools-Macros-Security menu options. This is **not the recommended option** for running in a production environment.

For more information in obtaining a digital certificate please consult Microsoft Office 2000/Visual Basic Programmer’s Guide — Part 4: Chapter 17 (Using Digital Certificates to Produce Trusted Solution).

You must close Outlook and re-open it before the security setting takes effect. This is because the VBA project was not signed. Since we know this is a test environment and the macro written is safe we can click the *Enable Macros* button.

Using the Email module

DB2 Records Manager provides a seamless e-Records solution for Microsoft® Outlook 2000. The IBM DB2 Records Manager Outlook module lets you:

- Declare e-mail messages as corporate records
- Provide classification information either manually or through an auto-classification rule.
- Store the e-mail and all attachments in the corporate repository.

The IBM DB2 Records Manager Outlook module provides full DoD 5015.2 compliancy including:

- Expansion of distribution lists
- The ability to file an e-mail message and it’s attachments:
  - as a single record
  - as separate records (linked)
  - both as a single record and each attachment as a separate record (linked)
- Captures all necessary transmission and receipt data.
- Does not allow the modification of transmission and receipt data.

Declaring email messages

DB2 Records Manager e-mail module lets you easily declare e-mail messages as corporate records. When you declare an e-mail message, you can include attachments with it.

Your administrator is responsible for creating a custom e-mail file plan component (record type) that has the fields relevant to e-mail messages. You must also have the proper permissions to access the e-mail and attachment. Contact your records administrator if you are having problems declaring e-mail messages.

E-mail messages without attachments

The following procedures show you how to declare an e-mail message with or without an attachment.

To declare an e-mail message:

1. Select the e-mail message you want to declare.
2. Click **Declare**.
3. Log on to DB2 Records Manager (if not already logged on).
4. Fill out the profile for the e-mail message. Your records administrator has set up the e-mail profile you see. All data fields that were captured from the e-mail records are read only and displayed in grey.
5. Click**Browse**to navigate to the location in the file plan where you want to file the e-mail.
6. Click **OK**.

Note: If you want to view the original e-mail message, got to the location in the file plan where you filed it.

Email messages with attachments

You can declare an e-mail message with attachments in three ways: as a single record, as separate records (linked), and both as a single record and as separate records (linked).

Declare as a single record:

1. Select the e-mail message you want to declare.
2. Click **Declare**.
3. Log on to DB2 Records Manager.
4. Click **Single Record**, and then click **OK**.
5. Fill out the profile for the e-mail message.
6. Click **Browse** to navigate to the location in the file plan where you want to file the e-mail.
7. Click **OK**.

Declare both as single and separate records:

1. Select the e-mail message you want to declare.
2. Click **Declare**.
3. Log on to DB2 Records Manager.
4. Click **Both**.
5. Fill out the profile for the e-mail message.
6. Click **Browse** to navigate to the location in the file plan where you want to file the e-mail.

7. Click **OK**.
8. Fill out the profile for the attachment.
9. Click **Browse** to navigate to the location in the file plan where you want to file the attachment.
10. Click **OK**.
11. Repeat until you have filed all attachments.

Glossary

A

accession. Involves the permanent transfer of a record and its metadata to another authority that assumes responsibility and ownership of the record.

advanced search. A search that generates a report based on system, custom file plan components, and file plan structure.

API. Application Programming Interface

application programming interface. A software interface that enables applications to communicate with each other. An API is the set of programming language constructs or statements that can be coded in an application program to obtain the specific functions and services provided by the underlying licensed program. The IBM Records Manager API provides server components for the host application to access IBM Records Manager. You can embed IBM Records Manager into any line-of-business application. A programmer can also use the API to modify, enhance, customize, or completely re-write the existing IBM Records Manager Administrator user interface.

archive. Persistent storage used for long-term information retention, typically very inexpensive for each stored unit and slow to access, and often in a different geographic location to protect against equipment failures and natural disasters.

attribute. A unit of data that describes a certain characteristic or property of an object.

B

bar code. A code used for identification purposes. In IBM Records Manager, applying pre-printed bar codes to items simplifies the file plan administration process. Users add new file plan components by scanning the items directly into the file plan.

binary large object. A sequence of bytes with a size ranging from 0 bytes to 2 gigabytes. This string does not have an associated code page and character set. Image, audio, and video objects are stored in BLOBs.

C

character large object (CLOB). A sequence of characters (single-byte, multibyte, or both) up to 2 gigabytes. A CLOB can store large text objects. Also called a character large object string. Compare to binary large object (BLOB).

charge-out. Checking out a component from the file plan. A charged-out, component is locked.

classify. A method of assigning retention and disposition rules to records. Depending on the particular implementation, it can be manual or process-driven. You can present users with a list of allowable file codes from a drop-down list (manual classification). Ideally, the desktop process or application can automate classification by triggering a file code selection from a property or characteristic of the process or application.

client application. An application written with the Content Manager APIs to customize a user interface.

CLOB. See character large object.

common search. A set of frequently used searches that you can easily execute from Search-Common. The searches you can execute in Search-Common are Audit, Reservation, Charge Out, User/Group, and Life Cycle Code.

component definition. See file plan component definition.

Cut-off. Breaking or ending files at regular intervals, usually at the close of a fiscal or calendar year, to permit their disposal, or to transfer complete blocks or segments.

D

DAO. Data access objects. They are object created with Visual Basic.

data types. A definition of a set of data. In IBM Records Manager, there are eight data types available for attributes: String, Binary, Boolean, Date, Date-Time, Double, Integer, and Character Large Object (CLOB).

declare. To designate that a particular document is a corporate record. Once declared as a corporate record, edit and delete control of the document is passed from the user to the record keeping process, as administered by the corporate records management professionals. As a record, a document can only be modified or deleted by the records management process, not by the end user. Users must be aware of those documents that are records (declared), versus those that are not yet declared. Declaration can be manual whereby the user decides when to declare, and then sets a property or selects a menu option to declare the document. Alternatively, it can be and automated process whereby specifying a certain property triggers the automatic declaration of the record.

descriptor. See security descriptor.

disposal authority. A code or rule for approving the disposal of certain records.

disposition. The last stage in the record life cycle. Disposing a file plan component (either accession or destruction) also disposes its descendants.

document. A document managed by the host application (any form or format), an email message or attachment, a document created within a desktop application such as MicroSoft Word, regardless of the format. There are two types of document: electronic and non-electronic. An electronic document is stored in electronic format and it can be read. If declared as a record, an electronic document becomes a managed record. A non-electronic physical object can take on many forms (such as maps, paper, VHS video tapes, and CDs). You cannot record the physical object using the same method as electronic documents; however, you can store its descriptive metadata, and then track this information within IBM Records Manager (a profile). If declared as a record, a non-electronic object becomes a managed record.

E

exclusive relationship. A relationship that is exclusive within its view. An exclusive relationship can only exist where there are several relationships that have the same source. This kind of relationship determines the types of components to allow in a relationship with respect to its existing members. For example, a file component can have any number of files (as children), however, if one of those files contains folders, that file is the end of a branch and it can contain only folders.

F

file plan. An organization will have a common classification scheme for the entire organization, called a file plan. The file plan is typically a hierarchical set of subjects or business activities. Each node or subject file is annotated with a unique code called a file code. A given file code refers to a specific subject file within the file plan. Each subject file has an official retention rule (when, why, and how to delete) assigned to it. Each record must be assigned a file code that matches the appropriate subject file with in the file plan.

file plan administration. The design and administration of a corporate file plan. The records manager can design file plan components (classes of file plan objects such as files, records, and folders), and then define the attributes of these classes and their relationships (for example, files can contain files, records, and folders). Various views of the file plan may be defined. For instance, a warehouse view might present a view of the physical folders in the organization, whereas a numeric view might present the sorted numeric structure for maintenance purposes. The records manager can create pick lists enforcing consistency within the file plan, component profiles that define the characteristics of the file plan, and default values to simplify daily file creation tasks. Policies, permissions, and suspensions can be assigned to file plan objects.

file plan component. The classification of file plan objects, such as files, records, and folders.

file plan component definition. A declaration that the specific type of file plan component will exist within the file plan. After you define a file plan component definition, an unlimited number of actual file plan components of that declared type can exist within the file plan. A file plan component definition is a meta-object, used to declare the type (either record or component) of the actual components.

file plan management. The process of designing, building, and maintaining a file plan.

file plan relationship definition. The relationship of components within the file plan. For example, a folder can contain files, records, and other folders.

file plan view. A collection of relationships between components that comprise the file plan. In the same way that a view in a relational database is a collection of joined tables that comprise a schema. File plan views give each component in the file plan a context. No file plan components can exist outside a view. Every file plan component must be in at least one view (Hierarchical, Link, and Set).

FPC. See file plan component.

H

hierarchical view. A hierarchical views represent a tree-like structure in a parent and child relationship. Hierarchical views can also represent containment (for example, a box can contain a folder). You can have as many hierarchical views in a file plan as you require, but you must have at least one hierarchical view in a file plan.

host. An application that uses IBM DB2 Records Manager to provide life cycle retention management. The responsibilities of the host application are to generate electronic information, to provide tools to manipulate that data, and maintain a repository to store the information.

host application. Business software application into which you embed IBM DB2 Records Manager.

host configuration. Host configuration lets an integrator register a business application as the host with IBM DB2 Records Manager. The integrator registers a business application by specifying information about their business application into which IBM DB2 Records Manager Administrator is integrated.

I

inheritance. The passing of class resources or attributes from a parent class to a child class.

IRM. IBM Records Manager

J

JDBC. Java database connectivity

Java Virtual Machine. Interprets compiled Java binary code for a computer's processor so that it can perform a Java program's instructions.

L

life cycle. A collection of phases through which any file plan component managed as a record must transit before it is disposed. A life cycle can consist of one or more phases; each phase lasting specific duration and denoting records management activity that must be performed at the beginning, or at the end of the phase. These phases comprise the life cycle duration.

life cycle code. A life cycle rule applied to a file plan component.

life cycle event. IBM Records Manager logs the following file plan component events as they occur: a component transitions to another phase, a component is disposed of (destroyed or accessioned), and a component fails to transition.

life cycle inheritance rules. When a file plan component does not have its own life cycle code, it inherits it from its closest ancestor in its primary view.

life cycle management. The records life cycle is the life span of a record from its creation, or to its final disposition. Typically, it is described in three stages: creation, maintenance and use, and final disposition. IBM DB2 Records Manager applies management to all three stages. With e-records, the records manager can create and maintain the official rules that determine when to destroy (or permanently keep) electronic records, as well as record and enforce any conditions that apply to destruction (for example, to destroy two years following contract completion). Finally, the records manager can carry out the physical destruction of electronic records, maintaining a legal audit file.

life cycle phase. A life cycle consists of one or more phases; each phase lasting specific duration and specifying records management activity to perform at the beginning, or at the end of the phase. These phases comprise the duration of a life cycle.

life cycle operations. The process of executing the rules that govern the life cycles of components (the transitioning of file plan components through their life cycles). After file plan components transition through all phases, they are ready for disposition.

life cycle rule. A rule that determine the following items: Time - How much time a component spends in any one phase of its life cycle. Security - Whether a component's security changes as it transitions from one phase to another in its life cycle. Disposal - How a component is disposed of when it completes the last phase of its life cycle. Cut off - Whether a component is cut-off when it enters a phase in its life cycle. Close - Whether a component is closed when it enters a phase in its life cycle. Interim transfer - Whether a component undergoes an interim transfer when it enters a phase in its life cycle. Begin Life Cycle When Superseded - Sets a file plan component to begin its life cycle when it is replaced by a new version. Event-Based Disposition - Sets disposition to be event based instead of time based.

life cycle suspensions. The suspension of a file plan component. If a file plan component does not qualify for transitioning, it will remain in its current life cycle phase until the removal of the suspension.

link view. A collection of unidirectional peer-to -peer type relationships. You can use a link view to establish a one-way relationship between two file plan component types. For example, a cross-reference link between two documents where two file plan components are cross-referenced to each other. There is no hierarchy between these documents. Users are aware of the existence of one document because it is cross-referenced to another.

logic extension class. Classes let you apply business rules to file plan components. You apply the business rules by associating logic extension classes with file plan component definition types and, then executing them.

M

metadata. In IBM DB2 Records Manager, metadata is a detailed profile that provides information about the content of a record, and it describes other characteristics about a record.

migration. The process by which you move a file plan component from one physical location to another.

O

ORB. Object Request Broker acts as a “broker” between the client request for a service from a component, and the completion of the request.

P

paging block size. A value that restricts the number of search results that display on a page.

partition. A set of access rules that restrict user actions, at the system or component level.

partitioned component. The sub-division of a file plan component into parts, separated by date. When IBM Records Manager creates an instance of a component, it automatically creates an initial partition (part) for that component. When users add records to the component, IBM Records Manager automatically inserts the records into the current part, until a new partition is created for the component. When a new partition is created, IBM Records Manager closes the initial part, and the new part receives any new records (opening a new part automatically closes the preceding part).

permissions. Permissions define what an individual user or group can do to a specific file plan component, such as a filing or a record. Permissions relate who can do what, and where in the file plan. Internally, the relationship between the who, the what, and the where, is called an access control policy.

phase. See life cycle phase.

pick list. Pick lists let you define values a user can select from a pre-defined list of choices. The IBM DB2 Records Manager pick list feature lets you create, edit, and delete pick lists and assign them to both file plan components and non-file plan components, such as users and groups.

primary view. A primary view provides a path for a file plan component to inherit properties that are not specifically set for that file plan component, a unique way to navigate to the file plan component, and a security context for the file plan component. It is a mechanism by which a file plan component inherits its inheritable properties (hierarchical view). Every file plan component gains its context within the file plan by belonging to at least one view.

profile. A data entry form containing attributes that users must specify for a component. Profiles restrict user access to certain fields on the form, as well as limiting the actions on these fields.

put away. The action of returning one or more charged out file plan components.

Q

query. A request for information from the database based on specific conditions.

R

record. Any form of recorded information that is under records management control. Records are either physical or electronic. Records can be any of the following types: Document - A document that was declared as a record. Once declared as a record, the document is under records management control. Folder - A physical folder containing documents. You can declare individual documents within the folder as records (declared as non-electronic documents). Box - A box containing paper documents. Usually contains folders, which are individually managed as records, but may alternatively contain records other than folders, such as loose documents about a specific subject. Non-electronic - A declared physical document of any form (such as maps, paper, VHS video tapes, and CDs). The physical object is not recorded in electronic form; however, you can use IBM Records Manager to store descriptive metadata about the objects, and track that information within the objects profile. If declared as a record, a physical object becomes a managed record. A document (electronic or non-electronic) is not considered a record until it is declared.

records management. The administrative infrastructure represents the tasks that the records manager performs on the entire organization's collection of declared records. End users never see this process; it conducted within the Records Manager Administration Client (a browser-based web application). Records management consists of the following broad activities; file plan administration, records security control, life cycle management, and reporting.

relationship definition. See file plan relationship definition.

repository. A physical storage area for documents and electronic records. Refers to the Host Application's repository.

reservation. A request by a user to borrow a file plan component on a future date. A file plan component could be a document, box, folder, or any other item you can deliver.

retention rules. The set of rules which specify how long to keep (retention) records, and what to do with them at the end of their life cycle (disposition)

retention schedule. See retention rules.

RMA. See records management application.

root view. The root is the top of any hierarchical file plan view. The root file plan component definition is a system object that you cannot edit or delete. You use the root file plan component definition in hierarchical relationships (relationship types that belong to hierarchical views) as the default. Every hierarchical view must have the root file plan definition as its root.

S

security descriptor. A series of words (from a common collection of words) allocated to file plan components and users, or to file plan components and groups. Security descriptors provide you with enhanced access control.

set view. A type of relationship that contains an ordered number of components that are independent of each other. Unlike the hierarchy and link views, a set does do not have a direction. Because an ordinal value describes the order of the records, sets provide you with version management capabilities for your records.

simple search. A search that generates a report for one or more fields in a custom file plan component. A simple search has three parts: scope, search details, and report output options.

SQL. Structure Query Language, SQL is an American National Standards Institute. standard computer language for accessing and manipulating database systems. SQL statements are used to retrieve and update data in a database.

suspend. A suspended file plan component no longer qualifies for transition in the current phase of its life cycle. When you suspended a file plan component, it remains in its current life cycle phase until the removal of the suspension.

system component definitions. Component definitions that represent business objects used specifically by IBM Records Manager. The system components included with IBM Records Manager are not the file plan components in the file plan hierarchy; they are required for the file plan to function, such as life cycle codes, user accounts, and group accounts.

V

view. See file plan view, hierarchical view, primary view, set view, and link view.

W

WSDL. Web Services Description Language. It is an XML based language used to describe the services you offer. WSDL is derived from SOAP and from the IBM Network Accessible Service Specification Language.

Notices

IBM may not offer the products, services, or features discussed in this document in some countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation Licensing
2-31 Roppongi 3-chome, Minato-ku Tokyo 106, Japan

Licensing

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS"WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
J74/G4
555 Bailey Avenue
San Jose, CA 95141
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Portions of this product were developed by The Apache Software Foundation (http://www.apache.org/) Copyright © 1999 The Apache Software Foundation. All rights reserved.

THE LOG4J, XERCES, XALAN SOFTWARE ARE PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL IBM OR THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The following terms apply to the LOG4J, XERCES, XALAN components:

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the above disclaimer in the documentation and/or other materials provided with the distribution.

The end-user documentation included with the redistribution, if any, must include the following acknowledgment: "This product includes software developed by the Apache Software Foundation (http://www.apache.org/)." Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.

The names "log4j, xerces, xalan" and "Apache Software Foundation" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org.

Products derived from this software may not be called "Apache", nor may "Apache" appear in their name, without prior written permission of the Apache Software Foundation.

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries or both:

IBM

DB2

WebSphere

Intel and Pentium are trademarks or registered trademarks of Intel Corporation in the United States, other countries, or both.

Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation in the United States, other countries, or both.

Index

Printed in USA