IBM DB2 Records Manager

Designing a DoD 5015.2 Compliant Solution

Version 3 Release 1

SC18-7717-00

IBM DB2 Records Manager

Designing a DoD 5015.2 Compliant Solution

Version 3 Release 1

SC18-7717-00

Notices:

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

First Edition (September 2003)

This edition applies to Version 3 Release 1 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' when setting up 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 to be 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.

Who should use this guide

Use this guide if you are a Records Manager and are responsible forUnited States Department of Defense 5015.2 compliant solutions or if you are partner responsible for designing your own integrated solutions.

How to use this guide

The following conventions are used in this guide:

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.

Make sure to examine the Records Manager readme file for additional information. See install-directory/readme.txt where *install-directory* is the directory in which you installed the 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/:

IBM DB2 Records Manager Concepts Guide	GC18-7575-00
IBM DB2 Records Manager Planning and Installation Guide	GC18-7578-00
IBM DB2 Records Manager Technical Reference	SC18-7573-00
IBM DB2 Records Manager User's Guide	SC18-7572-00
IBM DB2 Records Manager Designing a DoD 5015.2 Compliant Solution	SC18-7717-00

Related Publications

The following publication contains information related to Records Manager for the DB2 Web site at

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

- DB2 Universal Database™

How to send your comments

Your feedback helps IBM to provide quality information. Send any comments that you have about his book or 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

  You can use the page to enter and send comments.
- Send your comments by e-mail to comments@vnet.ibm.com. Be sure to include the name and part number of the book (if applicable). If you are commenting on specific text, please include the location of the text (for example, a chapter and section title, a table number, a page number, or a help topic title).

Chapter 2. Introduction

If you want to have your Host application certified as DoD 5015.2 compliant you can use the "DoD 5015.2" development model. A DoD 5015.2 certified product must meet all of the mandatory requirements. This development model requires more effort on the part of the Host application developers. The resulting product can be certified compliant with the DoD 5015.2 standard and placed on the compliant application roster.

A DoD 5015.2 compliant solution offers the same benefits as the e-Records Enabled solution but adheres to the more stringent DoD 5015.2 requirements. In terms of functionality both types of solutions offer life-cycle records retention capability. The difference is that DoD 5015.2 spells out *precisely* how this will be provided to the end-user.

The DoD database

Records Managers that want their electronic record management information system to comply with the DoD 5015.2 standards, can use the sample DoD database provided to help prepare.

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 enusure that the database meets your requirements. It is not meant to be a final and complete database. It is meant as a template to assist in the certification process. For more information refer to the IBM DB2 Records Manager Toolkit and the Records Management Application Compliance Testing Program at http://jitc.fhu.disa.mil/recmgt/

The DoD Logic Extensions

The DB2 Records Manager logic extensions are necessary for developing a DoD compliant database. Logic extensions allow you to add custom logic to selected file plan component methods.

The concept of logic extensions is to allow your application developers to modify the behavior of the IBM DB2 Records Manager business objects. This allows for flexibility in the business model.

To accomplish this, the DB2 Records Manager uses a simple listener pattern for each business object that is to be modified

For more information refer to the IBM DB2 Records Manager Toolkit.

Outlook Extensions

The IBM DB2 Records Manager provides a seamless e-Records solution for Microsoft Outlook 2000. You can file an e-mail message and its attachments as;

- a single record
- separate record (linked)
- both as a single records and each attachment as a separate record (linked)

The Outlook Extensions contain modules for storing and describing e-mail 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 SOAP Toolkit 3.0.

You must manually install the IRM DB2 Outlook e-mail macro into Outlook 2000.

The Outlook extensions allow you to

- declare e-mail messages as corporate records
- classify information either manually or through an auto-classify rule
- store the e-mail and all attachments in the corporate repository

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

Chapter 3. Designing a DoD 5015.2 Compliant Solution

If you want to build a solution that can be certified compliant with the for electronic records management, you will have to provide some additional functionality in your solution above and beyond the “eRecords enabled” solution requirements.

This chapter discusses what those requirements are and how you can meet them. Note that this document discusses one approach to meeting the requirements. However, you may wish to take a different approach. The requirements can be met in many different ways. Again, there is no single correct way to meet the requirements.

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.

There are two documents that outline the DoD 5015.2 requirements and how to meet them. One is the DoD 5015.2 baseline requirements document, the second is the DoD 5015.2 test cases. Both of these documents are available on the DoD web site. You should review and be very familiar with these documents.

http://jitc.fhu.disa.mil/recmgt/

The requirements outline the specific requirements that must be met to ensure DoD 5015.2 compliance. Chapter 4 “DoD 5015.2 Requirements Summary for Partners” on page 33in this document, describes who is responsible for satisfying each of the DoD 5015.2 Requirements -- either DB2 Records Manager or the host application.

The DoD 5015.2 test cases describe the specific test scenarios that the DoD testing team run against your solution to confirm compliance. Note that the DB2 Records Manager web administrator satisfies the majority of the test cases. This document describes how your application must be designed to meet the remaining host specific test cases.

The following sections 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 filters out all of the requirements satisfied by DB2 Records Manager or that are not relevant to designing your integration with the DB2 Records Manager. It explains only the work that must be done by the host application to ensure compliance. Under each test step or group of test steps with in test case, you will see text in the following format:

The quick brown fox jumps over the lazy dog.

This text has been extracted from the original test cases document. It is added by IBM to help you prepare for the test by explaining what you must do to pass the test. Wherever a specific task case or test step is extracted, this section will provide

an explanation describing which application (DB2 Records Manager or your application) is responsible for carrying out the test. Where your application is the one responsible four carrying out the test, specific examples and instructions will be provided.

Because you are integrating your product with DB2 Records Manager, you will inevitably be required to write software code. This section will also provide useful insight that will help effectively design and write your integration with DB2 Records Manager.

Note: In many test cases, the test is self-describing or what you must do is obvious. In those cases, we have provided no additional comments.

A Possible Integration Strategy

There is an indefinite number of strategies you can employ to integrate your product with the DB2 Records Manager. This document illustrates one possible strategy. The strategy that we will assume throughout this document is as follows:

1. The 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). Therefore your application will continue to be the host for all the documents and records. You will simply "register" your documents as records with DB2 Records Manager.
2. The DB2 Records Manager is designed to provide users with a single point of login using a common user account and password with their 'home' application. This generally is the host application also. Therefore all user and group management functions will continue to reside within the host application. Users and groups will be managed within the host application and PROXIES for those users will be created within DB2 Records Manager. There will be no need for duplicate users and groups to be specified in each of the two applications. This is discussed in detail in Test Section 3.
3. All records related metadata will be stored and managed using DB2 Records Manager. The existing document related metadata in the host application does not need to change significantly. You must however add a field to store the unique record IDs for any document declared as a record.
4. All document filing templates and profiles will be managed using DB2 Records Manager. The host is responsible to RENDER those profiles and apply those templates whenever a user in the host application declares a document as a record (you can use the DB2 Records Manager API to obtain the document profiles and templates). The user will then supply the relevant records related metadata or the data can be retrieved from corresponding fields in the document metadata from the host.
5. A key aspect of declaring a document as a record is to identify the file (aka record series) to which the record belongs. The DB2 Records Manager provides extensive functionality in its API for navigating the file plan, however the host must provide a user interface. This user interface must also support the ability to list only file code for which a user has filing access.
6. You must also impose the same security regime on a document in your host application as the corresponding record profile in DB2 Records Manager. In other words, if a record profile in DB2 Records Manager is designated to have a restricted access for only 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 (here

after 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 DB2 Records Manager, that is where security is applied and is inherited by all records beneath it. If you do not implement this approach, there will effectively be a back door in your application granting unauthorized users access to records in the host to which they do not have access in DB2 Records Manager.

7. The host application must create an implementation of the HostInterface interface and register that implementation with DB2 Records Manager. For more information refer to the IBM DB2 Utility Reference3 in the online API Reference.

The DB2 Records Manager's DOD enabled Database[1]

You can install DB2 Records Manager's DOD enabled database to save you the time and effort of setting up the necessary data for performing the test. (The DB2 Records Manager DoD enabled Database is part of the toolkit.)

It consists of the following file plan views: DOD 5015.2, Quick Lists, and Cross Reference[2]. It also consists of the following file plan component definitions: Series, Files, Folders, Documents, QuickLists, and Email. These are described as follows.

File Plan Views

File Plan View: DOD 5015.2

This view is hierarchical and represents the file plan view that organizes the main objects that make up the file plan. These include the following file plan component definitions: Series, Files, Folders, and Documents. These are described below. Included in the descriptions, are the file plan component definition id's for each of the main types of objects. You will need to know the ID's when writing your programs with the DB2 Records Manager API.

Series The broadest category of classification. In the file plan design, Series have one relationship definition that relates them to Files where the Series is the Source (i.e. the parent in a hierarchical view) and the files are the Targets (i.e. the children in a hierarchical view).

Files The next level of classification. In DOD 5015.2 terminology they are called Record Category. Files can be further sub-divided into sub-files. Files can also contain Folders and Documents. Files have three possible relationships where the file is the Source: 1) files (as the Source/Parent) can be related to other files (as the Targets/Children) in a hierarchical progression from broadest categories to most specific categories; 2) files (as the Source/Parent) can be related to folders (as the Target/Child); 3) and finally files (as the Source/Parent) can be related to documents (as the Target/Child).

Folders Represent mechanisms for organizing documents within a file. Folders can only contain documents, and therefore they support only one relationship definition: a folder (as the source/parent) can be related documents (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 File or Folder. Documents are the lowest level of the file plan and therefore there are no relationships defined below them.

Versions In DOD requirements each record can have many versions. There is a DOD requirements that states: when a user is presented with a specific version of a record in a result list and the user attempts to view or retrieve that record, the system must present the user with a message informing them whether there are more recent versions of that record, it must present them with a list of the more recent versions, and allow them to select one of those versions instead of the one they originally tried to retrieve.

File Plan View: Quick Lists

This file plan view was added to meet a specific requirement of the Standard whereby users, when filing a document, will only see the set of files into which they have access to file documents. There are numerous approaches that can be taken to meet this requirement. The one discussed here is a simple manual approach whereby an authorized user groups a number of existing files into a quick list and then grants individual users access to the quick list. When a user files the document, instead of navigating the entire file plan, the file plan browser (explained later) only allows users to navigate to quick lists.

This file plan view is also hierarchical and consists of one file plan component definition also named QuickList.

Quick List A quick list is a file plan component definition used to define groupings of files. The file plan component definition id of a quick list is 5. There are no other relationships with which a quick list participates within the quick list view.

File Plan View: Quick List Jump

The name may leave a bit to be desired but it gets the point across. A quick list jump view is a non-hierarchical view that contains no inherent file plan components. Instead it is a view containing a single relationship whose sole purpose is to link any particular file in the DOD 5015.2 view with one or more Quick Lists in the Quick List view. The rationale for creating this additional view is as follows: According to the DB2 Records Manager concepts discussed in the *DB2 Records Manager Concepts Guide*, any file plan component can participate in any number of file plan views (hierarchical or not). However, a file plan component cannot have more than one parent in any one hierarchical view. In order to allow any file to be linked to more than one quick list (something which is very likely) the relationships between the quick list and file cannot be hierarchical. This file plan view therefore allows any quick list to be related to any number of files and vice versa.

File Plan View: Cross Reference

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.

User Defined Business Logic

This section is based on Revision 7.3 (September 2002) DoD 5015.2-STD RMA COMPLIANCE TEST PROCEDURES. Several test cases in this document are based on 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 supplied by IBM to work with DB2 Records Manager

IBM will supply you with the following logic extensions:

IRMDodDocumentExtension.jar

The com.ibm.gre.dod.extensionDocumentListener and the com.ibm.gre.dod.extension.SupercedeLogicExtension classes are contained in the IRMDodDocumentExtension.jar that is included in the toolkit folder. (See: Toolkit\DoD 5015.2\LogicExtensions.)

These are the logic extensions that you must install into the DB2 Records Manager Extensions facility for the Document file plan component. For details on how to create and edit logic extensions in the DB2 Records Manager, consult the *DB2 Records Manager User Guide*.

The DocumentListener logic extension contains the special logic attached to the "Supplemental Markings" field and 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, the "Supplemental Markings" field and the "Project" field.

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

The SupercedeLogicExtension contains the special logic associated with the test case where an email must be sent to a particular user when a record is superseded. It will send out a notification E-mail when a record is superseded in a category that has a final disposition of ″Destroy when superseded or obsolete.″

In order for these logic extensions to work properly, you must have created ALL the custom fields specified in the accompaning ReadMe.txt files.

ProjectAccess.bat

This logic extension is used to meet the requirement specified in Test Cases associated with Custom Field name "Project". The ProjectAccess.bat is included in the toolkit folder. (See: Toolkit\DoD 5015.2\LogicExtensions.)

To meet this requirement simply RUN this batch file. It will generate an HTML based report that meets the above requirement. You must edit this logic extension to supply it with the UserID, Password, and DBAlias that it can use to log into the DB2 Records Manager to generate the necessary reports. For details on how to install and configure this logic extension in the DB2 Records Manager, consult the Readme located in the Toolkit\DoD 5015.2\LogicExtensions directory.

In order for this logic extension to work properly you must have created ALL the custom fields specified in the following section using EXACTLY the same name, datatype and length.

VitalRecords.bat

This logic extension is used to meet the following requirement specified in Test Cases associated with Custom Field Name "Vital Records". To meet this requirement you should create a scheduled task using the Windows 2000 scheduled task wizard. This macro will send an email to the designated users informing them of the VITAL records that are due for review.

For details on how to install and configure this logic extension in the DB2 Records Manager, consult the Readme located in the Toolkit\DoD 5015.2\LogicExtensions directory.

In order for this logic extension to work properly you must have created ALL the custom fields specified in the following section using EXACTLY the same name, datatype and length.

Users must not change the following; These are defaulted to strUserID= "Administrator", strPassword = "cronos", and database= "". It is recommended that you NOT change the user from the "administrator".

During the Tests

Testing the special logic associated with the field named "Supplemental Marking"

At the beginning of a test case make sure that the Document extension and the Email extension are enabled. These extensions will trigger each time a document or email are added or updated. They will update the ACL assigned to each document based on the document's original ACL, their assigned Supplemental Markings and their Assigned Projects.

Testing the special logic associated with the field named "Project"

There are two special tests for this. The first test is regarding the Access Restrictions placed on a document based on its assigned project. At the beginning of the test case make sure that the Document extension and the Email extension are enabled. These extensions will trigger each time a document or email are added or updated. These extensions will 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 is regarding the generation of a special report, namely: "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.)." This test is carried out by simply RUNNING (double clicking) the "projectAccess.bat" batch file.

Testing the Special Logic Associated With the Field Named Vital Record

You can simply double click on the batch file named VitalRecords.bat. This will show the result immediately. Otherwise you can use the Windows 2000 task scheduler to create a scheduled task running this job.

DOD 5015.2 Test Cases

TEST SECTION 2: TEST READINESS EVALUATION

TEST CASE #2-1: EVALUATE SET UP

This section is meant to provide the testers with insight into your readiness to be tested. In the past, the DOD testers have encountered situations where they have stopped the test and failed the vendors due to the vendor's lack of readiness. DB2 Records Manager helps you a long way towards being ready by providing a ready-built file plan, users, groups, profiles, defaults, etc. that you can use for your certification. These are available from the IBM DB2 Toolkit. If, however, you are using your own users and groups, document profiles (for example, forms used to capture document and record metadata), within your own application, or you have not installed the DB2 Records Manager DOD compliant database from the toolkit. You must have the features described here-in built and ready to demonstrate your readiness for the test.

Verify user accounts: Note that the DB2 Records Manager's DOD-ready database comes with these users predefined, however they are considered LOCAL groups. If you are using your own groups, you must ensure that these groups are defined in your host and also are imported into the DB2 Records Manager.

For a list of user accounts that will be used during testing consult the Test Cases Document. You must pay particular attention to column 4 with the heading Clearance, Supplemental Markings. Clearance does not apply to these tests. Supplemental Markings must exist as a multi valued field in the user's DB2 Records Manager account profile. This field will be used throughout the test in conjunction with an equivalent field on the document profile to ascertain the ability to write user defined logic to control access to a record.

Verify Groups: Note that the DB2 Records Manager's DOD-ready database comes with these groups predefined, however they are considered LOCAL groups. If you are using your own groups, you must ensure that these groups are defined in your host and also are imported into the DB2 Records Manager.

For a list of these groups refer to 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 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 the DB2 Records Manager. You must ensure that your application either provides these fields and maps them directly to the DB2 Records Manager or, upon declaration of a record, that you provide a data entry form allowing the user to supply the information to the DB2 Records Manager.

For a list of the standard data elements refer to the Test Cases Document.

Verify Groups: Verify data entry templates. For a pairing, verify host system data entry templates.

These are all provided by the 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 the DB2 Records Manager.

For a list of the data entry templates refer to the Test Cases Document.

Verify the file plan: The necessary file plan components are supplied in the DB2 Records Manager's DOD-ready database.

Verify Access and Limitations: The Test Cases Document outlines 4 types of access limitation. These are:

1. Restrictions on users ability to file records into portions of the file plan.
2. Restrictions on groups ability to file records into portions of the file plan.
3. Restrictions on users ability to search for and retrieve records from portions of the file plan.
4. Restrictions on 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 have been specified in the DB2 Records Manager's DOD-ready database. However these permissions are specified for the pre-defined local users and groups only. If you will be using your own HOST users and groups, you will need to apply these permissions for your groups as well.

TEST CASE #2-2: NEGATIVE TESTING

The following five users can be logged on and tested simultaneously: Schlotterer, Tassotti, Dale, Finnegan and Christy.

These "negative" tests all involve users attempting to use functions to which the users should not have access. Five separate users are used to test these, however the tests are identical for all the users. We will therefore document only the procedures for the first user.

This section will point out only those tests that may involve the host.

Attempt to access the functions to manage users.

Attempt to access the functions to manage groups.

Because user and group management is carried out in the host application, these tests will also be carried out in the host application. A portion of these tests will also be carried out in DB2 Records Manager. These include the tests 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 the DB2 Records Manager, therefore these tests will be carried out in the DB2 Records Manager. If however, some of the data elements are defined within your host application, such tests may be carried out 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 the data elements for records. Because these exist only in the DB2 Records Manager, these tests will be carried out there.

Attempt to access the functions to create/modify data entry templates including default organization wide values.

Retrieve a record, attempt to modify the content, attempt to modify the metadata, attempt

to change the folder/record category. (The user should be allowed to enter event dates to the metadata.)
Attempt to change the metadata of a filed record. (As a privileged user, Schlotterer 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 still considered record meta-data and is subject to the same permissions as the DB2 Records Manager-specific record meta-data. In order to determine whether any specific user is allowed to alter the record meta-data, you should access the ACL (access control list) of the record from the DB2 Records Manager. See documentation for **FilePlanComponentControllerEJB.getEffectiveUserPermissionsList** in the *IBM DB2 Records Manager API Reference*. If your host maintains its own ACL, the DB2 Records Manager can automatically inform it whenever the permissions change that affect one or more documents stored in your host. The host can then 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. (The user should only see the 210, 165, 25, and 5 series, and 71-1 Folders 1 and 2.)

When filing a record, the standard requires that only files to which the user has access to file documents are visible. The rational for this is that when filing documents, there is no point in showing a user files to which the user does not have the permissions to file documents. Once again there are many approaches that can be taken to meet this requirement.

A simple approach is to create user filing lists. These are lists of files to which individual users have access to file records. You can use the DB2 Records Manager's file plan design features to enable these lists (Note: before proceeding to implement this approach you should read the *DB2 Records Manager Concepts Guide*). The DB2 Records Manager DOD 5015.2 enabled database that contains the file plan you can use and all the necessary data elements also contains a second file plan view named QuickLists. This file plan view is an alternate hierarchical view that enables you to group files. You can create these quick lists for different users and add only the files to which they have filing access. In the navigator you build that allows users to locate the files to file documents, you can, instead of navigating the entire file plan, restrict them to ONLY the QuickLists.

Using that database and the constructs within it you can limit the browser to show only the Quick List File Plan View. Using the fact that the ID for the quick list file plan view is 2, you can for the root of your navigator call,

```
FilePlanComponentControllerEJB.getTargetList(nViewID=2,nFilePlanComponentID=0, ...)
```

This will return the complete list of quicklists within the quick list view.

To show the list of files associated with each quicklist, knowing that they will be related to the quick list within the quick list jump view (whose ID = 5), your code can then call,

```
filePlanComponentControllerEJV.getTargetList(nViewID=5,nFilePlanComponentID=x, ...)
```

Where x is the ID of any Quick List.

This is a very manual and redundant approach however it is simple and it meets the requirement. A more 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. You can

use the DB2 Records Manager API function named, **filePlanComponentControllerEJB.getEffectiveUserPermissionsList** to get the set of permissions any particular user has for a file.

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

Attempt a "select all" search. Note what categories/folders are returned. (The user should only see 710, 210, 165, 25, and 5 series, and 71-1 Folders 1 and 2.)

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 the DB2 Records Manager. Otherwise there will be a back door in your host application granting users the access to documents that they should not see. You can use any of the following methods to obtain the permissions for a particular user for a document:

filePlanComponentControllerEJB.getAllowedHostActionList,

filePlanComponentControllerEJB.getAllowedLocalActionList,

filePlanComponentControllerEJB.getEffectiveUserPermissionsActionList.

For details on these functions consult the *DB2 Records Manager API Reference and Progamming Guide*.

The above approach assumes that prior to showing a user the results of any search, you will query the 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. An alternative is to synchronize your record's ACL with the one in the DB2 Records Manager. You must implement the **onPermissionUpdate** method from the HostInterface. You can also use he following methods

```
filePlanComponentControllerEJB.getFilePlan
ComponentsWithChangedPermissions
```

and

```
filePlanComponentControllerEJB.getNewPermissions
ForFilePlanComponents
```

to determine the Records with permissions that have changed. For more details refer to the API Reference.

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

Maintenance of shortened quick pick lists, which are user specific subsets of master pick lists, is tested using the DB2 Records Manager. For details consult the *DB2 Records Manager Records User Guide*. However, your host must be able to RENDER quick pick lists.

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.)

The creation and maintenance of data entry templates and defaults is normally carried out in the DB2 Records Manager. Therefore, this test can be carried out there. However, the host application must be able to RENDER those templates and apply the defaults within its own application

TEST SECTION 3: USER MANAGEMENT

TEST CASE #3-1: CREATE USER ACCOUNTS

The DB2 Records Manager allows you use your own users and groups defined in your own product as users and groups within DB2 Records Manager as well. You can use DB2 Records Manager to create proxies of your application user and group

accounts and to grant those proxies explicit permissions for perform actions within DB2 Records Manager. This allows you to manage your users and groups in one application (not two). It also allows you to avoid compelling your users to have separate log-in names for each application.

This document assumes that user and group management will be performed within your application and that only proxies of your application's user and group accounts will be added to the DB2 Records Manager database. To do this you will have implemented the **getGroupList** and **getUserList** functions found in the hostInterface interface. Any application integrating with DB2 Records Manager must implement the hostInterface and register it with DB2 Records Manager. For details on the hostInterface consult the *DB2 Records Manager API Reference*[3].

Once a proxy for a user account has been added to the DB2 Records Manager database, that user will be able to access DB2 Records Manager features directly from within the Host application. They must still log into DB2 Records Manager, however they can be logged in, using a special function belonging to the LoginManagerEJB class of the DB2 Records Manager API. This function, named hostLogin, assumes a user is logging in from the host application, and that the user is a valid user in the host application.

A user with a proxy in DB2 Records Manager can also log directly into DB2 Records Manager. In this case, the user must supply their credentials and the host application to which they belong to the DB2 Records Manager. DB2 Records Manager will use these credentials to validate the user with the host application before granting the user a session.
Add the following user accounts: (For a pairing add the accounts to both host system and RMA.

a.	*User name:*	*Don Damson*
b.	*ID:*	*damson*
c.	*Password:*	*tackle1*
d.	*Clearance:*	*CONFIDENTIAL*
e.	*Supplemental Markings:*	*NOFORN*
a.	*User name:*	*Bruce King*
b.	*ID:*	*kingbru*
c.	*Password:*	*tackle2*
d	*Clearance:*	*SECRET*
e.	*Supplemental Markings:*	*none*

Because the Host application is the one in which user and group management is performed you will add these users and groups into the Host application. You will then "import" them into DB2 Records Manager. In order to allow your users and groups to be imported you must first have implemented the getUserList and getGroupList methods of hostInterface interface for your application. The hostInterface interface is described in detail in the *DB2 Records Manager API Reference*. Once you have implemented this interface you can use DB2 Records Manager to directly import your users (see the *DB2 Records Manager Records User's Guide* for instructions on how to import users).

3. NB — in order for this mechanism to work successfully, the host application must provide a unique immutable identifier for each user and group. This immutable identifier is used to "point" DB2 Records Manager back to the actual account in the Host application. The Login Name or User Name cannot be used if they are not immutable.

Supplemental Markings is a field used in the user and group profiles in the DB2 Records Manager in conjunction with the DB2 Records Manager's macro facility to control access to records. You must supply the Supplemental Marking values to the user's profile in the DB2 Records Manager AFTER you have imported the users from the host application.

Delete the King user account.

Attempt to log on using King's (deleted) account. Verify that logon is unsuccessful.

You can delete the King user account from within the host application. You can then also programmatically delete the King proxy in DB2 Records Manager using the DB2 Records Manager API. You can call the method fetchExternalUser within the userGroup class to the get the user's DB2 Records Manager ID and then call Delete to the delete the user.

However, if you don't delete the King proxy from DB2 Records Manager, King will no longer be able to log into the host application and so will also not be able to access DB2 Records Manager using the LoginManager.EJB.hostLogin method. King will also not be able to log directly into DB2 Records Manager even though King's proxy is still in DB2 Records Manager. This is due to the fact that DB2 Records Manager will first validate King's credentials with the Host Application. Because the King account has been deleted within the host application, King will not validate and so DB2 Records Manager will not allow King to complete the login.

Note that you must implement the hostInterface.ValidateUser method (refer to the API Reference) in such a way that the method will accept the user's valid credentials and validate 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 DB2 Records Manager database, DB2 Records Manager will grant the user a session.

Modify the following user account as shown:

		Old account:	**Modified account:**
a,	User name:	Don Adamson	(no change)
b,	ID:	adamson	(no change)
c,	Password:	tackle1	tackle4

Log in using Adamson's new password. Verify access to file and retrieve records, including supplemental markings. (Also include classified records if classified is implemented).

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

Because the Host application is the one in which user and group management is performed, modifying user accounts is also performed within the host. Within 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 so there is no need to resynchronize accounts between the Host and DB2 Records Manager. This greatly reduces the complexity inherent in maintaining separate user accounts in two applications. However, the name Bruce King and the login id kingbru remain in the DB2 Records Manager. You may wish to extend the integration between the DB2 Records Manager and your host application to automatically change the login id and the name programmatically upon a change occurring in the host. Otherwise these can be changed manually by an administrator in the DB2 Records Manager.

Generate a printed listing of all users for reference during the test. Verify the printed output against the expected results, based on Table 2-1.1. and the steps above (additional user).

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 DB2 Records Manager reporting facility.

TEST CASE #3-2: CREATE USER GROUPS

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 DB2 Records Manager, see the above discussion related to users.

In addition, this document assumes that all user-group membership is maintained in the host application. DB2 Records Manager is designed to support the management of host users and groups within the host application and to incorporate the user-group membership when the user logs in. Each time a Host based user logs in, whether by logging in from the host application using LoginManagerEJB.hostLogin or by logging directly into DB2 Records Manager, DB2 Records Manager will query the host application to provide the list of groups to which the user belongs. DB2 Records Manager will then create a temporary user-group membership between the user that is logging in and each group to which the user belongs. This temporary membership will expire once the user logs out. This allows host applications to assign users to groups without regard for DB2 Records Manager, and to know that when the user is accessing DB2 Records Manager features, they will have the rights and permissions from all the groups to which they belong.

When a user is logging into DB2 Records Manager from the host application, the method to use is the hostLogin method of the LoginManager class in the DB2 Records Manager API. On of the parameters in that method is the Group List to which the user belongs. For details consult the *DB2 Records Manager API Reference* for the LoginManagerEJB class.

When a user is logging into DB2 Records Manager directly, using the DB2 Records Manager own user login form, need only provide their valid credentials. Once DB2 Records Manager has validated the user's credentials (using the validateUser method of the HostInterface), DB2 Records Manager will then call upon the host to provide a list of groups to which the user belongs. For details consult the *DB2 Records Manager API Reference* descriptions for the HostInterface interface.

Note that while 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 (in reality their proxies) are assigned to host groups (in reality their proxies) using DB2 Records Manager own 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 show up in the host application.

Add a "Test Officers" user group. Add Adamson to the "Test Officers" group.

Assign functional access to Test Officers group. If classified is implemented assign privileged user access to Adamson as security representative for Test Officers. Note how security functional access can be distributed across a hierarchy.

Log in as Adamson to verify access. Logout.

Because the host application is the one in which user and group management is performed, you will add these users and groups into the host application. You

will then "import" them into DB2 Records Manager. In order to allow your users and groups to be imported you must first have implemented the getUserList and getGroupList methods of hostInterface interface for your application. The HostInterface interface is described in detail in the *DB2 Records Manager API Reference*. Once you have implemented this interface you can use DB2 Records Manager to directly import your groups (see the *DB2 Records Manager Records User's Guide* for instructions on how to import groups).

Functional Access within the context of this certification means access to features in the DB2 Records Manager. Once the Test Officers Group from the host application have been imported into the DB2 Records Manager, assigning it functional access is performed within the DB2 Records Manager. Adamson can then directly log into the DB2 Records Manager to test functional access.

Delete Earl Holloway from the "Finance" group, and add him to the "Test Officers" group.

You can perform this step within the host application. Because DB2 Records Manager does not maintain user-group membership information, and this information is only created at login time, and lasts only for the duration of the session, the next time Earl logs into DB2 Records Manager he will NOT be a member of the "Finance" group. Of course you can also add users to groups in the DB2 Records Manager. Its up to you how you want to organize the test.

Change the name of the "Analysts" group to "Engineering".

This step is performed in the Host Application, where groups are maintained. Note however that changing the name in the Host will NOT result in the name of the group Proxy to be changed in the DB2 Records Manager. You must do that programmatically from within the host when the name changes. Or you can delete the Proxy from the DB2 Records Manager and re-import it from the host with the new name.

Delete the Test Officers group. Note whether system warns that users exist in this group.

This step is performed in the Host Application, where groups are maintained. Make sure that the host application presents a warning if the group contains members. Note, however, that deleting the Group in the host will not automatically result in the group proxy being deleted in the DB2 Records Manager. You must do that programmatically from within the Host Application. Or you can delete the proxy within the DB2 Records Manager manually.

Generate a printed listing of all groups for reference during the test. Verify the printed output against the expected 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 only using the DB2 Records Manager reporting facility.

TEST SECTION 4: SETUP FILE PLAN

TEST CASE #4-1: BUILD FILE PLAN INFRASTRUCTURE

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

However, DB2 Records Manager also provides an off-the-shelf web-based user interface that allows you to 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 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 DB2 Records Manager's own profile rendering mechanisms. These also set the default values.

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

For this test you will log directly into DB2 Records Manager using the off-the-shelf web-based User Interface. You must specify the Login ID (christyd), the Password (monkey2), and the name of your host application as you named it when you configured your host application. See the relevant section in this guide.

For detailed instructions regarding the remaining test steps in this test case, consult the relevant sections of the *DB2 Records Manager Records User's Guide*.

A significant change to Version 6.6 of the test cases is the inclusion of user defined logic on several fields in the DB2 Records Manager. This 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.

These include the fields named Supplemental Markings and Project. Both these fields are custom defined fields in the DB2 Records Manager. Throughout the test cases you will find references to user defined logic attached to these fields. For the sake of simplicity, we have gathered all the references from throughout the document and placed them here as part of the 'infrastructure' of the file plan. The rationale for this is that part of the infrastructure of the file plan is the user defined business logic that extends the functionality of the DB2 Records Manager.

Test Case 4-1:
Add user-defined field, "Project Name" (text) to the metadata set. For pairing, take necessary steps in host system as well as in RMA. Perform necessary mapping to ensure data entered in host system is properly passed to RMA.
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 only using the DB2 Records Manager reporting facility.Define master selection lists/control tables/pick lists for user defined file plan components (Project Name); modify existing lists if this capability is provided by the RMA under test.
Specify default values for filing documents, if this capability is provided (not a mandatory requirement). Project Name default is "unassigned." Modify existing defaults.
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.).

Test Case 4-3:
Constrain access based on Project Name. Each user or group should have a limited sub-set of Project Names that they will assign to records. They should only be allowed to search and retrieve on those Project Names to which they have access.

Test Case 4-3-a: "Add access control logic to the Supplemental Markings field, such that a user would need, in his profile, all the values entered for a record in order to access (search and retrieve) that record."

The test cases do contain the following explicit references to the Supplemental Markings field

Test Case 2-1:
Verify user accounts.
Verify supplemental markings pick list includes NOFORN and NOCONTRACT. If classified is implemented, include FORMERLY RESTRICTED DATA and RESTRICTED DATA.

Test Case 4-1:
Add FOUO to Supplemental Markings picklist.

Test Case 6-1:
Finnegan searches for FOUO documents. Note the record ID of a document. Dale uses this document in Test Case #7-1 Screening/Editing.
Edwards searches for FOUO documents. (Edwards and Finnegan are in the same group.) She should not see any.

Test Case 7-1:
Edit the Supplemental Markings field of a classified record in 5-1. Access an unclassified document with no supplemental markings. (From Edward's negative testing.) Change markings to FOUO. Save the record.
Access an unclassified record marked FOUO. (From Finnegan's search testing.) Change supplemental markings to blank. Save the record.
Special Logic Associated with Field Named "Vital Records".

Test Case 4-1:
Add logic to send e-mail to Dan Christy when a vital record folder is due for review. This should be an action that routinely monitors the vital record review dates and not just implemented when a folder is "touched."

In order to help you pass these test cases, IBM has developed the following logic extensions that can operate from within the DB2 Records Manager logic extension environment:

com.ibm.gre.dod.extension.DocumentListener

The com.ibm.gre.dod.extension.DocumentListener is contained in the IRMDodDocumentExtension.jar that is included in the toolkit folder, (\Toolkit\DOD5015.2\DodDLogicExtensions.)

This is a extension that you must install into the DB2 Records Manager Extensions facility for the Document file plan component. For details on how to create and edit extensions in the DB2 Records Manager, consult the *DB2 Records Manager Programming Guide*. This extension contains the special logic attached to the "Supplemental Markings" field and to the "Project" field. It runs each time a document is added or updated and it updates the ACL for the document based on the document's original ACL, the "Supplemental Markings" field and the "Project" field.

In order for this extension to work properly, you must have created ALL the custom fields specified in the following section using EXACTLY the same name, datatype and length.

This Extension should also be used in the email file plan component.

ProjectReportMacro.vbs

This macro is used to meet the requirement specified in Test Case 4-1 Step. To meet this requirement simply RUN this macro. It will generate an HTML based report that meets the above requirement. You must edit this macro to supply it with the UserID, Password, and DBAlias that it can use to log into the DB2 Records Manager to generate the necessary reports.

You can only run this macro on a computer that has either the DB2 Records Manager or the DB2 Records Manager COM client proxy installed.

In order for this macro to work properly you must have created ALL the custom fields specified in the following section using EXACTLY the same name, datatype and length.

VitalRecordMacro.vbs

This macro is used to meet the following requirement specified in Test Case 4-1 Step 4.12. To meet this requirement you should create a scheduled task using the Windows 2000 scheduled task wizard. This macro will send an email to the designated users informing them of the VITAL records that are due for review.

You can only run this macro on a computer that has either the DB2 Records Manager or the DB2 Records Manager COM client proxy installed and also has Microsoft Outlook 2000 installed.

In order for this macro to work properly you must have created ALL the custom fields specified in the following section using EXACTLY the same name, datatype and length.

The DB2 Records Manager UserID, Password and database default to strUserID= “Administrator”, strPassword = “cronos”, and database= “”. It is recommended that you NOT change the user from the “administrator”.

During the Tests:

Testing The Special Logic Associated With The Field Named “Supplemental Marking”:

At the beginning of the test case 4-1 make sure that the com.ibm.gre.dod.extension.DocumentListener is enabled. These logic extensions will trigger each time a document or email is added or updated. These logic extensions will update the ACL assigned to each document based on the document’s original ACL, their assigned Supplemental Markings and their Assigned Projects.

Testing The Special Logic Associated With The Field Named “Project”:

There are two special tests for this. The first test is regarding the Access Restrictions placed on a document based on its assigned project. At the beginning of the test case 4-1 make sure that the Document extension and the Email extension are enabled. These extensions will start each time a document or email is added or updated. They will 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 is regarding the generation of a special report, namely: “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.).”This test is carried out by simply RUNNING (double clicking) the “ProjectReportMacro.vbs”visual basic script file.

Testing The Special Logic Associated With The Field Named Vital Record:

You can simply double click on the visual basic script file named

VitalRecordMacro.vbs. This will show the result immediately. Otherwise you can use the Windows 2000 task scheduler to create a scheduled task running this job.

TEST CASE #4-2: CREATE/MAINTAIN RECORD CATEGORIES AND FOLDERS

These test steps can be completed using DB2 Records Manager's own user interface. For details regarding how to carry out these steps, consult the *DB2 Records Manager User's Guide*..

TEST CASE #4-3: LIMIT RECORD CATEGORIES AND FOLDERS

These test steps can be completed using DB2 Records Manager's own user interface. For details regarding how to carry out these steps, consult the sections in the *DB2 Records Manager User's Guide,* regarding applying permissions to file plan components.

TEST SECTION 5: FILING

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

The nature of product pairings is that host application users will be logged into 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 ASP 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.

TEST CASE #5-1: 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. Note the user name or ID of each of the four users below:

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

Table 1. DOD 5-1.1—Editing Permissions for Record METAData — During Filing. In this table the following fields have been added as user defined fields in the DOD enable database for DB2 Records Manager: Supplemental Marking 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 DB2 Records Manager Custom Field creation mechanism.

Requirement Paragraph	Metadata Field	Indicate Auto-capture or Manual Entry	Editing Allowed?
C2.2.3.2.1	Unique Record Identifier	Auto	No
C2.2.3.2.2	Supplemental Marking List		
C2.2.3.2.3	Subject		
C2.2.3.2.4	Media Type		
C2.2.3.2.5	Format		
C2.2.3.2.6	Date Filed	N/A	No
C2.2.3.2.7	Publication Date		
C2.2.3.2.8	Date Received		
C2.2.3.2.9	Author or Originator		
C2.2.3.2.10	Addressee(s)		
C2.2.3.2.11	Other Addressee(s)		
C2.2.3.2.12	Originating Organization		
C2.2.3.2.13	Location of Record		
C2.2.3.2.14	Vital Record Indicator		
C2.2.3.2.15	Vital Record Review and Update Cycle Period		
C2.2.3.2.16	User-Defined Fields		

This document assumes that all records related metadata listed in the above table will exist in the DB2 Records Manager database. Some of these fields may already exist in the host application. DOD testers will be looking for an automatic mapping of these field values into the corresponding fields in the DB2 Records Manager records metadata. 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 profile and you support the inclusion of both sets of meta-data in a report.

The simplest solution is to capture all records related data in 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 DB2 Records Manager. Once 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 (Tassotti, modem.dif, 5-1 and 25-1z).

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, 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 simply 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 get back 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 the **hostInterface.onPermissionChange** interface definition and configured your host entry in the DB2 Records Manager to receive notification each time permissions change in the DB2 Records Manager that could alter the permissions. Your implementation of hostInterface.onPermissionChange must perform/call the following functions:

1. Call **FilePlanComponentControllerEJB.getFilePlanComponentField(filePlanComponentFId, "ACPID", false)**. This will return an identifier uniquely identifying the Access Control List. Also call **FilePlanComponentControllerEJB.getPermissionList**. This will return in XML form the complete Access Control List that you must use to alter the permission on your document.
2. Call **FilePlanComponentControllerEJB.getRegisteredPermissionDescendants**. This will return a list of file plan components in your host that are descendants of the file plan component whose permissions were changed, and therefore derive their permissions from it.
3. For each Item in this list call **FilePlanComponentControllerEJB.getAllowedHostActionList**. If this list contains more than one entry then this item represents a multiply registered document. For all entries in this list you must create a single virtual access control list and apply it to your document. To do this call FilePlanComponentControllerEJB.getPermissionList for each entry in this list and merge the separate access control lists into a single one that is the intersection of all of them.

   Designate at least one document as a vital record and add the monthly review dates. Use category 165-1-16a, user Schlotterer, file Sunday.dot.

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. (The file can go into Schlotterer, 71-1, Folder 1.).

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. Note records on spreadsheet. (Christy, category 710-1, help.doc and help2.doc.)

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. (Dale, category 5-10a, outcomes.doc and outcomes.pdf.)

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 hot to bundle the various renditions of a record. You can inform the IRM when 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. (Tassotti)

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 the same techniques described above. It will be your application that handles the incrementing of version numbers.

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. In other words 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.

Date Processing . Enter the following values as Publication Date in the record metadata. Note if Declassify On date changes to date + 10 years if classified is implemented note that declassified date is a valid date.

Table 2. DOD Table 5-1.2—Entering Document Creation Dates

Date	Valid	Invalid	Notes
31 Jan 1800	ã		
29 Feb 1900		ã	Not a Leap Year
29 Feb 1956	ã		Leap Year
29 Feb 2000	ã		Leap Year
29 Feb 2100		ã	Not a Leap Year
29 Feb 2104	ã		Leap Year

TEST CASE #5-2: FILE E-MAIL 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. Note that this assumes that all records related metadata will be stored in DB2 Records Manager. If some metadata 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.

TEST CASE #5-3: 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 DB2 Records Manager. This document assumes that you will use DB2 Records Manager to file non-electronic records. For details on how to carry out these test steps, consult the *User's Guide..*

TEST SECTION 6: SEARCHING FOR AND RETRIEVING RECORDS

TEST CASE #6-1: 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 ... namely: 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 simply log into DB2 Records Manager using the DB2 Records Manager login screen. The user can then execute the searches completely within DB2 Records Manager. However, they will be using the 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 will be as follows:

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, "What's new and summary of requirements for partners," on page 33 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 Dan Christy (a user in your host application) executes a search within your host application (if your host supports searching), and Dan Christy does not have access to view records located in file 1-1b, then the result list within your application MUST NOT include any documents declared as records and filed in file 1-1b. The DB2 Records Manager has several methods that allow you to query on the security of any individual record. These methods include **getAllowedHostActions** and **getAllowedLocalActions**. 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 happens 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 retieve records from a host application, you must implement the following methods in the remote host interface

1. getContentList
2. open contentStreamFromRead
3. ContentStreamRead

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 theDB2 Records Manger User'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

TEST CASE#7-1: 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.

TEST CASE #7-2: 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 in-situ. Altering the duration of a life cycle or changing the disposition effectively re-schedules any records to which that life cycle code applies.

TEST CASE #7-3: 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 how 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

TEST CASE #8-1: 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.

TEST CASE #8-2: 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 that 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. In such a case 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, HostInterface.destroy, or HostInterface.accession 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. (25-1z and 5-1)

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, DB2 Records Manager will instruct 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.

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

TEST CASE #9-1: 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. The DB2 Records Manager allows you to record auditable events that occur in your host application. This relevant method is named ToolsControllerEJB.addAuditEntry.

For details on what constitutes an auditable event, consult the *DB2 Records Manager Records User's Guide*.

TEST CASE #9-2: 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.

TEST CASE #10-1: 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 In the end.

TEST CASE #10-2: USER INTERFACE

These features are not mandatory.

TEST CASE #10-3: SUPPORT FOR RM PROCESS

These features are supported in the DB2 Records Manager.

TEST CASE #10-4: 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*.

TEST CASE #10-5: BACKWARDS COMPATABILITY

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

Chapter 4. What's new and summary of requirements for partners

Improved Support

Improved support for DoD extensions for partners (e.g. view host document).

DoD 5015.2 Requirements Summary for Partners

Table 3. C2.1. GENERAL REQUIREMENTS

DoD 5015.2 Requirements	Host Requirements
C3.1. Managing Records. RMAs shall manage records in accordance with this Standard, regardless of storage media or other characteristics [44 U.S.C. 3103 and 36 CFR 1222.10;].	This is a general requirement that will be met automatically when the detailed requirements, described below, are met.
C2.1.2. Accommodating Dates and Date Logic. RMAs shall correctly accommodate and process information that contains dates in current, previous, and future centuries [FIPS 4-2;]. 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 (e.g., 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, "DoD Data Administration Procedures,". 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 certified 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.

Table 3. C2.1. GENERAL REQUIREMENTS (continued)

DoD 5015.2 Requirements	Host Requirements
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 4. C2.2. DETAILED REQUIREMENTS

DoD 5015.2 Requirements	Host Requirements
C2.2.1. Implementing File Plans. C2.3.1. 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) Mandatory file plan components are shown in Table C2.3.1. 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 must ensure population of the associated data structure with non-null values. For fields that are not mandatory in the Data Collection column, RMAs must behave in a predictable manner as a result of queries or other operations. 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. C2.3.1.1., Record Category Name, Mandatory C2.3.1.2., Record Category Identifier, Mandatory, RMAs shall ensure unique C2.3.1.3., Record Category Description, Mandatory C2.3.1.4., Disposition Instructions, Mandatory C2.3.1.5., Disposition Authority, Mandatory C2.3.1.6, Permanent Record Indicator, Mandatory C2.3.1.7., Vital Record Indicator, Mandatory C2.3.1.8., Vital Record Review and Update Cycle Period, Mandatory, conditional on Vital Record Indicator C2.3.1.9., User Definable Fields, Optional	DB2 Records Manager provides full functionality for maintain 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

Table 4. C2.2. DETAILED REQUIREMENTS (continued)

DoD 5015.2 Requirements	Host Requirements
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 C2.3.1
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). Mandatory record folder components are shown in Table C2.2.1.3. 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 must ensure population of the associated data structure with non null values. For fields that are not mandatory in the Data Collection column, RMAs must behave in a predictable manner as a result of queries or other operations. C2.2.1.3.1., Record Folders, Optional C2.2.1.3.1.1., Folder Name, Mandatory C2.2.1.3.1.2., Folder Unique Identifier, Mandatory, RMAs shall ensure unique C2.2.1.3.1.3., Location, Mandatory if not in RMA repository C2.2.1.3.1.4., Vital Record Indicator, Mandatory, inherited from Record Category (can be changed by authorized individuals) C2.2.1.3.1.5., Vital Record Review and Update Cycle Period, Mandatory, conditional on Vital Record Indicator C2.2.1.3.1.6., Supplemental Marking List, Optional C2.2.1.3.1.7., User Definable Fields, Optional	See C2.3.1
C2.2.1.4. RMAs shall ensure that identifiers (e.g. folder identifiers, record category identifiers, etc) are unique so that ambiguous assignments, links, or associations cannot occur.	See C2.3.1

Table 4. 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 user to define and attach user-defined business rules and/or access logic to any metadata field including user-defined fields.	See C2.3.1
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 C2.3.1

Table 5. C2.2.2. Scheduling Records

DoD 5015.2 Requirements	Host Requirements
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. RMAs shall provide the capability for defining multiple phases 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
C2.2.2.2. 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: C2.2.2.2.1. Retention Period (e.g., fiscal year). C2.2.2.2.2. Disposition Action (interim transfer, accession, permanent, or destroy). C2.2.2.2.3. Interim Transfer or Accession Location (if applicable).	See C2.2.2.1

Table 5. C2.2.2. Scheduling Records (continued)

DoD 5015.2 Requirements	Host Requirements
C2.2.2.3. RMAs shall, as a minimum, be capable of scheduling and rescheduling each of the following three types of cutoff and disposition instructions: C2.2.2.3.1. 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.). C2.2.2.3.2. 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). C2.2.2.3.3. 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 C2.2.2.1
C2.2.2.4. RMAs shall provide the capability to automatically calculate the complete life cycle, including intermediate phases, of record folders and records [RM Handbook;].	See C2.2.2.1
C2.2.2.5. RMAs shall provide the capability for rescheduling dispositions of record folders and/or records during any phase of their life cycle if an authorized user changes the disposition instructions. This requirement includes the capability to change the cutoff interval of disposition instructions and to change the retention period associated with a disposition.	See C2.2.2.1
C2.2.2.6. The RMA shall provide recalculation of the record lifecycle based on changes to any lifecycle date and set the filing status (i.e., open, closed) of the folder according to the business rules associated with date change(s).	See C2.2.2.1

Table 6. C2.2.3. Declaring and Filing Records

DoD 5015.2 Requirements	Host Requirements
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.	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 6. 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 7. 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 must 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.	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”.

Table 7. DOD C2.2.3.2. Record Metadata Components

Requirement	Record Metadata Component	Structure	Data Collection Required by User	Reference/Comment
	Record Identifiers, Markings, and Indicators			
C2.2.3.2.1.	Unique Record Identifier	Mandatory, system generated (All)	Mandatory (System Generated, not editable)	

Table 7. DOD C2.2.3.2. Record Metadata Components (continued)

Requirement	Record Metadata Component	Structure	Data Collection Required by User	Reference/Comment
C2.2.3.2.2.	Supplemental Marking List	Mandatory (All)	Mandatory (may be defaulted)	Multiple Supplemental Markings entry selections shall be supported [DCID 1/7, DoD 5210.83, DoD 5400.7-R, DoDD 5230.24, and DoD 5200.1-R; references]
	Record Descriptors			
C2.2.3.2.3.	Subject or Title	Mandatory (All)	Mandatory	[36 CFR 1234.22; reference]
C2.2.3.2.4.	Media Type	Mandatory (All)	Mandatory	[RMTF; reference]
C2.2.3.2.5.	Format	Mandatory (All)	Mandatory	[RMTF;]
	Record Dates			
C2.2.3.2.6.	Date Filed	Mandatory (All)	Mandatory (System Date, not editable)	[RMTF;]
C2.2.3.2.7.	Publication Date	Mandatory (All)	Mandatory	[36 CFR 1234.22; reference]
C2.2.3.2.8	Date Received	Mandatory	Optional	
	Record People and Organizations			
C2.2.3.2.9.	Author or Originator	Mandatory (All)	Mandatory	[36 CFR 1234.22; reference]
C2.2.3.2.10.	Addressee(s)	Mandatory (All)	Mandatory for correspondence	
C2.2.3.2.11.	Other Addressee(s)	Mandatory (All)	Mandatory for correspondence	[36 CFR 1234.22, EO 12958, 32 CFR 159a.21; references]
C2.2.3.2.12.	Originating Organization	Mandatory (All)	Mandatory	[36 CFR 1234.22; reference]
	Additional Metadata			
C2.2.3.2.13.	Location	Mandatory	Optional	[RMTF; reference]
C2.2.3.2.14.	Vital Record Indicator	Mandatory	Optional	[36 CFR 1236.20; reference]
C2.2.3.2.15.	Vital Record Review and Update Cycle Period	Mandatory, conditional on Vital Record Indicator	Mandatory, conditional on Vital Record Indicator	[36 CFR 1236.20; reference]

Table 7. DOD C2.2.3.2. Record Metadata Components (continued)

Requirement	Record Metadata Component	Structure	Data Collection Required by User	Reference/Comment
C2.2.3.2.16.	User-Defined Fields	Mandatory/ Undefined	Optional	Multiple User-Defined Fields shall be supported

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 7. 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 7, 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 7. 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 7, 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.	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.	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 7. 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 7, 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 7. 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 7, 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 [36 CFR 1222.50 and RMTF].	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 7. 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 7, then the host application must also provide the forms for entering the metadata.
C2.2.3.10. RMAs shall (for all records) capture 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 [36 CFR 1234.22 and 36 CFR 1222.50].	See C2.2.3.7
C2.2.3.11. For records that are being filed via 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 autofiling, RMAs shall provide the user the option of editing the record metadata prior to filing. 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.	See C2.2.3.7

DoD 5015.2 Requirements	Host Requirements
C2.2.3.12. 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 [36 CFR 1234.22; reference].	See C2.2.3.3
C2.2.3.13. RMAs shall provide the capability to view, save, or print the metadata associated with a specified record or set of records.	See C2.2.3.6
C2.2.3.14. 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*
C2.2.3.15. 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.
C2.2.3.16. 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.	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.
C2.2.3.17. RMAs shall provide the capability to link original superseded records to their successor records.	See C2.2.3.16
C2.2.3.18. 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.

DoD 5015.2 Requirements	Host Requirements
C2.2.3.19. 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.
C2.2.3.20. RMAs shall link the record metadata to the record so that it can be accessed for display, export, etc.].	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.
C2.2.3.21. 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 C2.2.3.7
C2.2.3.22. RMAs shall enforce data integrity, referential integrity, and relational integrity. RMAs shall provide the capability to automatically synchronize multiple databases and repositories.	
C2.2.3.23. 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 C2.2.3.7), the host must implement the ability to render quick-pick lists in the filing form.
C2.2.3.24. 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 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.

DoD 5015.2 Requirements	Host Requirements
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.	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 C2.2.4.2., if available from the e-mail system, as part of the record metadata when an e-mail message is filed as a RMAs shall provide the capability for editing Subject or Title, Author or Originator, Addressees, and the Other Addressees metadata fields prior to filing. All other fields are not editable. *The intelligent name[1] of the sender.*-RMAs shall automatically enter this data into the Author or Originator data field (C2.2.3.2.9.). *The intelligent name of all primary addressees (or distribution lists).*-RMAs shall automatically enter this data into the Addressee(s) data field of the record metadata (C2.2.3.2.10.). *The intelligent name of all other addressees (or distribution lists).*-RMAs shall automatically enter this data into the Other Addressee(s) data field (C2.2.3.2.11.). *The date and time the message was sent.*-RMAs shall automatically enter this data into the Publication Date data field (C2.2.3.2.7.). *For messages received, the date and time the message was received (if available).*-RMAs shall automatically enter this data (if available) into the Date Received data field (C2.2.3.2.8.). *The subject of the message.*-RMAs shall automatically enter this data into the Subject or Title data field of the record metadata (C2.2.3.2.3.). **Note:** 1. Intelligent names are clear, uncoded, identifications of the individual	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 7. 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.
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 7.	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.	

DoD 5015.2 Requirements	Host Requirements
C2.2.5.1. RMAs shall provide an interface to one or more repositories for storing electronic records. The RMAs shall prevent unauthorized access to the repository(ies)	Storing records is the responsibility of the host application.
C2.2.5.2. 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 C2.2.5.1
C2.2.5.3. RMAs shall allow only authorized individuals to move or delete records from the.	See C2.2.5.1
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.
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 Eligibility Date. C2.2.6.1.1.2. Disposition Action. C2.2.6.1.1.3. Current 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. Location. C2.2.6.1.1.9. 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 results 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.	

DoD 5015.2 Requirements	Host Requirements
C2.2.6.1.5. RMAs shall provide for sorting, viewing, saving, and printing lists of record folders and/or records that have no assigned disposition [RMTF; reference].	
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 users 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 [Part I: NARA Review; reference].	
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.
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 [RM Handbook;].	
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 [Part I: NARA Review;].	
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	
C2.2.6.4.2. RMAs shall provide a field for authorized individuals to enter the reason for freezing a record or record folder	

DoD 5015.2 Requirements	Host Requirements
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.	
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 records and metadata shall 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 functions Transfer and Accession. The host must implement these two functions. 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 (i.e. metadata) for non-electronic records such as paper documents, maps, books, etc... then it will be responsible to store and extract the metadata 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. 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.
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 refiled as a record.
C2.2.6.6. Destroying Records.	

DoD 5015.2 Requirements	Host Requirements
C2.2.6.6.1. RMAs shall identify and present the record folders and records, including record meta data, 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 Category with the longest retention period. Links to Record 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 'undeleted' 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	
C2.2.6.6.5. RMAs shall restrict the records destruction commands to authorized individuals.	
C2.2.6.6.6. RMAs shall provide documentation of destruction 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 refiled as a record.
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.	

DoD 5015.2 Requirements	Host Requirements
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 supporting using the IBM DB2 Records Manager reporting user interface. If DB2 Records Manager 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 7 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.	
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.	
C2.2.6.8.6. RMAs shall allow users the ability to search for null or undefined values.	

DoD 5015.2 Requirements	Host Requirements
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 [RMTF;].	
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.	
C2.2.7. Access Control. Table 8. summarizes requirements that refer to "authorized individuals" and offers additional information regarding example user type roles and 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. 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.

Table 8. DOD C2.2.7. Authorized User Requirements

Requirement	Application Administrator	Records Manager	Privileged User
C2.3.1. Create, edit, and delete file plan components and their identifiers.	Ensures that data structures are correctly installed and database links are in place	Enters file plan data	None
C2.2.1.2. Designate the metadata fields that are to be constrained to selection lists. Create and maintain selection lists (e.g., drop-down lists) for metadata items that are constrained to a pre-defined set of data.	Ensure database is correctly set up and installed	Define Lists	User abilities

Table 8. DOD C2.2.7. Authorized User Requirements (continued)

Requirement	Application Administrator	Records Manager	Privileged User
C2.2.1.3. Create, edit, and delete record folder components and their identifiers.	Ensures that data structures are correctly installed and database links are in place	Enters folder data	Enters folder data
C2.2.1.5. Define and attach user-defined business rules and/or access logic to metadata fields including user-defined fields.	Creates rules and connects them to fields.	Manually execute rules if necessary	None
C2.2.2.1. View, create, edit, and delete disposition schedule components of record categories.	Ensures that data structures are correctly installed and database links are in place	Enters disposition data, enters event data, closes folders.	Enters event data and closes folders.
C2.2.2.2. Define the cutoff criteria and, for each life cycle phase, the following disposition components for a record category . . .	Ensures that data structure is correctly installed and database links are in place	Enters criteria and phase information	None
C2.2.2.5. Change the disposition instructions.	None	Edits disposition information and manually executes rules necessary to reschedule	None
C2.2.3.3. Create, edit, and delete record metadata components, and their associated selection lists.	Ensures that data structure is correctly installed and database links are in place	Creates Selection Lists	Enters data (all users)
C2.2.3.4. Select where data collection for optional metadata fields is mandatory for a given organization.	During Setup	Advising	None
C2.2.3.7. Arrange record metadata components and user defined record components on data entry screens to be used for filing.	During Setup	Advising	None

Table 8. DOD C2.2.7. Authorized User Requirements (continued)

Requirement	Application Administrator	Records Manager	Privileged User
C2.2.3.12. Define and add user-defined metadata fields (e.g. project number, budget line) for site-specific requirements.	During Setup	Advising	None
C2.2.3.14. Limit the record folders and record categories presented to a user or workgroup.	Record Categories during setup	Record Folders	Record Folders
C2.2.3.15. Change a record folder or record category associated with a record.	As necessary	As necessary	None
C2.2.3.16. Change or delete links and associations.	Database is correctly installed and configured	Change links as necessary	Make Links
C2.2.3.21. Modify the metadata of stored records.	As necessary	Change data as necessary	Time-Event and Event folders
C2.2.5.3. Move or delete records from the repository.	As necessary	As necessary	None
C2.2.6.1.4. Indicate when the specified event has occurred for records and record folders with event and time-event driven dispositions.	Database setup	Link dispositions to record categories	Enter event information
C2.2.6.2.1. Close record folders to further filing after the specified event occurs.	As necessary	As necessary	As necessary
C2.2.6.2.2. Add records to a previously closed record folder or to reopen a previously closed record folder for additional public filing.	As necessary	As necessary	As necessary
C2.2.6.3.1. Approve cutoff.	As necessary	Routine work	None

Table 8. DOD C2.2.7. Authorized User Requirements (continued)

Requirement	Application Administrator	Records Manager	Privileged User
C2.2.6.3.2. Add records or make other alterations to record folders that have been cut off.	Database support	Enters limits	None
C2.2.6.4.1. Extend or suspend (freeze) the retention period of record folders or records beyond their scheduled disposition.	Database and business rules	Freezing/ Unfreezing	None
C2.2.6.4.2. Unfreeze capability.	Database and business rules	Freezing/ Unfreezing	None
C2.2.6.5.4. Delete the records and/or related metadata after successful transfer has been confirmed.	As necessary	As necessary	None
C2.2.6.6.2. Confirm the delete command, before the destruction operation is executed.	As necessary	As necessary	None
C2.2.6.6.4. Access to records destruction commands.	As necessary	As necessary	None
C2.2.6.7.1. Enter the Vital Records Review and Update Cycle Period when creating or updating the file plan.	Ensuring database structure is adequate and correctly installed	Enters cycling data	Cycles and Updates Records
C2.2.8.2. Determine which of the specified actions listed in C2.2.8.1. are audited.	Manage Audits	None	None
C2.2.8.3. Set up specialized reports to determine what level of access a user has, what records each user accessed, and what operations were performed on those records and associated metadata.	Create Reports	None	None
C2.2.8.6. Report audit information to authorized individuals.	Execute audit	None	None

Table 8. DOD C2.2.7. Authorized User Requirements (continued)

Requirement	Application Administrator	Records Manager	Privileged User
C2.2.8.8. Backup and remove audit files from the system.	Backup and remove Files	None	None
C3.2.1. (Optional) Make global changes to the record categories, record category identifiers, disposition instructions, disposition instruction identifiers, and originating organization.	As necessary	As necessary	None
C3.2.2. (Optional) Bulk load capability.	As Necessary	As Necessary	None

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. RMAs shall provide the capability for authorized users to define the minimum length of the Userid field 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 8 to individuals and to groups.	This is the responsibility of IBM DB2 Records Manager.

DoD 5015.2 Requirements	Host Requirements
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 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	This is a joint responsibility. The host application must inform DB2 Records Manager of any activities such as relating to the viewing, deleting, editing or copying of a record. Or changing user accounts.
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.

DoD 5015.2 Requirements	Host Requirements
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 (DBMS). 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 ensure data integrity by providing the capability to compile updates (records, metadata, and any other information required to access the records) to RMAs, 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.
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.

DoD 5015.2 Requirements	Host Requirements
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.

Chapter 5. IBM Outlook e-mail Module

IBM 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. Hooks 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 is displayed the first time. 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

Out-of-the-box, however, the Outlook e-mail Module is not complete. A couple of steps must be provided by the host application before the e-mail module is completely 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 (eg. Files).

      Now the Outlook e-Mail module should be operational. The reason that you must provide the previous three steps is that they are unique for each

partner's host application. The steps are clearly documented in the IRMMacros.bas file with Java 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.

e-Mail Module architecture

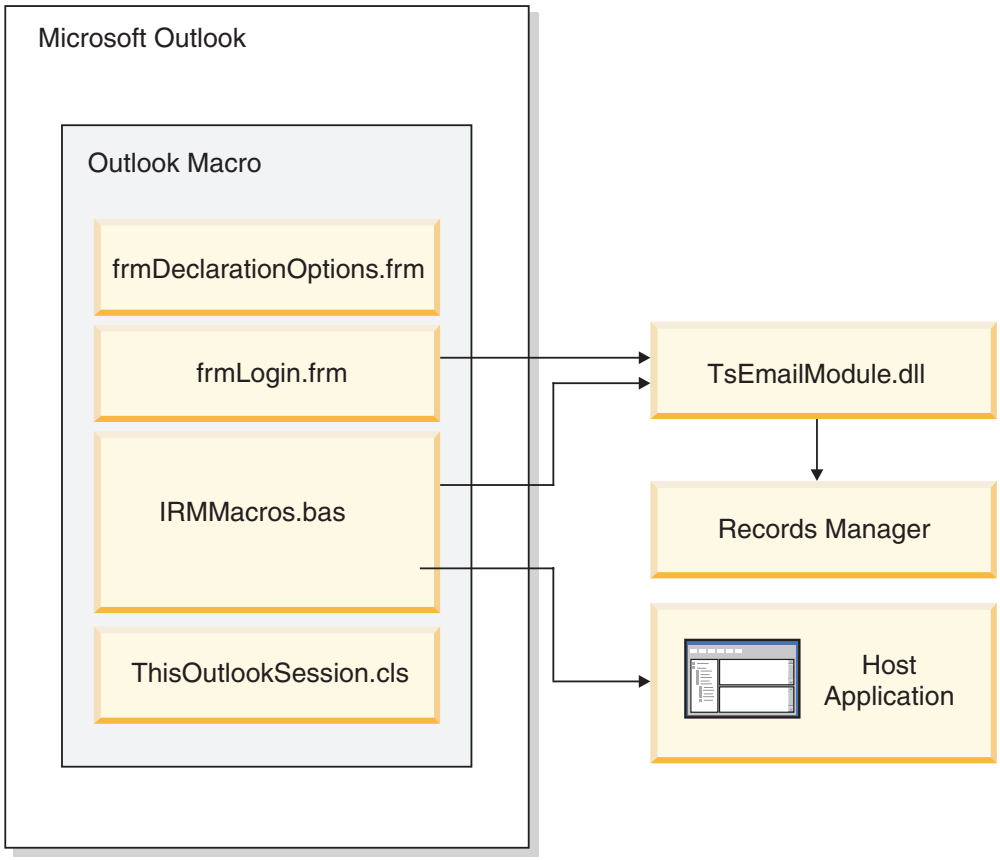
The next diagram illustrates how the IBM Outlook e-Mail module components interact. The main IBM outlook macro is loaded manually into Microsoft Outlook. It consists of:

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.

e-Mail 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
Version	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. DB2 Records Manager will store the attachment under 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
E-mail	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
CstFrom	String	
CstAddressees	String	
CstOtherRecipients	String	
CstEmailSentDate	String Or DATE	See readme notes YYYY-MM-DDTHH:mm:ssZ

Name	Type	Comments
CstEmailReceivedDate	String Or Date	See readme notes YYYY-MM-DDTHH:mm:ssZ

Once you have completed 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.

```
Public Const lEmailID As Long = 6
Public Const lAttachmentID As Long = 6
Public Const lCrossReferenceViewID As Long = 6
Public Const lVersionDefinitionID As Variant = 346
Public Const strServerURL As String = "http://<servername>:9080/IRMWebServices/servlet/rpcrouter"
```

e-Mail 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. Launch "Microsoft Outlook".
2. Open "Visual Basic Editor" from "Tools->Macros->Visual Basic Editor" or by AltF11.
3. Right Click on "Project1" project and select "Import File..." menu.
4. Navigate to the directory where DB2 Records Manager was 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" menu and setup project references.

    Note: **IRMProxy and IRMEmailModule.dll** are required. Please ensure that these are checked in the **References** dialog box.SOAP Toolkit 3.0 must be installed.

    Note: The preceding image is a close up of the References dialog box.
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 “Toolbars” tab and click “New” button.
18. Pick a name for a new button and click “OK”.
19. Select “Commands” tab.
20. In the “Categories” list select “Macros”
21. A list of available “Commands” should appear 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 “Visual Basic Editor”.
26. In “Project Explorer” expand “Modules” and double click on “IRMMacros” module.

Macro Security Issues

Note: If macro security is turned on with a security level of high, the macros will not work. Since this is just a test environment we will change the security setting to Medium. This can be done from Tools-Macros-Security menu options. Note 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 reopen 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 e-mail 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 e-mail 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.

E-mail 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

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.

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 (for example, name, address, age, and so forth) of an item, and which can be used to locate that item. An attribute has a type, which indicates the range of information stored by that attribute, and a value, which is within that range. For example, information about a file in a multimedia file system, such as title, running time, or encoding type (MPEG1, H.263, and so forth).

attribute group. Convenience grouping of one or more attributes.

B

base attributes . A set of indexes that is assigned to each object.

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.

BLOB. See binary large object

C

Class. In object-oriented design or programming, a model or template that can be instantiated to create objects with a common definition and therefore, common properties, operations, and behavior. An object is an instance of a class.

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

D

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

SOAP. Simple Object Access Protocol simple XML based protocol that is designed to exchange structured and typed information on the Web.

W

WSDL. Web Services Description Language. It is an XML based language. You use it to describe the services you offer and you provide the means to access the services electronically. WSDL is derived from SOAP and from IBM's Network Accessible Service Specification Language.

Index

Numerics

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W

X

Printed in USA

SC18-7717-00