

# iRIMS v9.0.5 by Open Text Corporation

---

## iRIMS Summary Report

The Joint Interoperability Test Command (JITC) tested Open Text Corporation's iRIMS v9.0.5, a stand-alone records management application (RMA) at the Open Text facility in Ottawa, Canada from 11 through 22 November 2002. The implementation was verified using version 6.6 of the Test Procedures and was compliant with DoD 5015.2-STD, dated June 2002. All mandatory requirements were satisfied.

In addition, JITC tested iRIMS v9.0.5 for compliance with Chapter 4, Management of Classified Records. All mandatory requirements of Chapter 4 were satisfied.

### TABLE OF CONTENTS

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

## 1. Product Identification

iRIMS v9.0.5, hereafter referred to as iRIMS, is a stand-alone RMA. iRIMS includes security features that can be used to handle the management of classified records. Organizations have the option of implementing iRIMS with or without using the security features.

The iRIMS software package, as tested, consisted of the following component programs and utilities:

- iRIMS v9.0.5, including:
  - iRIMS Navigator (Main user interface)
  - String Customizer Utility (Used for making changes to standard data element mapping.)
  - View Customizer Utility (Used to customize search screen layouts.)
  
- Crystal Reports (Must be purchased separately)\*

\*iRIMS ships with the run time version of Crystal Reports. Administrators who design report templates need to purchase the full version of Crystal Reports separately. iRIMS supports Crystal Reports Version 6,7 and 8.

## 2. Test Configuration

The baseline test configuration consisted of:

- One personal computer (PC) running the Microsoft (MS) Windows 2000 Advanced Server operating system (OS), MS SQL Server 2000, and iRIMS 9.0.5.
- One client PC running MS Windows 2000 Professional (SP3). Installed software included MS Office 2000 (SR1), MS Outlook 2000 (SR1), and iRIMS 9.0.5.
- One client PC running MS Windows XP (SP1). Installed software included MS Office XP Professional, MS Outlook 2002, and iRIMS 9.0.5

The baseline configuration for iRIMS was tested with the security features enabled.

In a subsequent configuration, iRIMS was also tested with the security features disabled.

In other configurations, JITC repeated the certification test using the Oracle 8.1.7 database.

Table 1 summarizes all tested configurations:

<b>Table 1 iRIMS Tested Configurations</b>			
<b>RMA</b>	<b>OS</b>	<b>DBMS</b>	<b>Note</b>
iRIMS with Security features enabled	Windows 2000 Advanced Server	SQL 2000	Baseline test
iRIMS with Security features enabled	Windows 2000 Server	Oracle 8.1.7	
iRIMS without Security features enabled	Windows 2000 Advanced Server	SQL 2000	
iRIMS without Security features enabled	Windows 2000 Server	Oracle 8.1.7	

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

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

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

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

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

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

iRIMS provides the capability to implement standard data. Records managers create data entry templates. They can assign default values to system native fields and pick lists to user-defined fields to assist the user in filling out the templates.

iRIMS can be configured with all the data elements as defined in DoD 5015.2-STD. The records manager can also configure iRIMS with additional fields for custom use. Custom fields are created and added to the data entry templates using the iRIMS Extender utility. Administrators can constrain the selection lists presented to users by using filters to partition access.

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

This is the first test for this product against version two of DoD 5015.2-STD<sup>1</sup>, therefore test data was not available to verify backwards compatibility.

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

Open Text provided the 508 Voluntary Product Accessibility Templates (VPATS) provided as Appendix C in the detailed test report. Open Text's VPATs are also available online at: <http://www.section508.gov/index.cfm?FuseAction=Search&SearchType=ListProductsCompany&companyid=729>

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

iRIMS provides the required capabilities for creating and maintaining disposition instructions and file plans. Disposition instructions are created separately and assigned to record plan components when creating the file plan categories. Subcomponents under that level inherit the same disposition instruction unless another disposition instruction is specified for that lower level component.

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

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

iRIMS automatically tracks the disposition schedules for screening and disposition processing. Records managers reschedule files by assigning a different disposition instruction to the file or altering the retention period (which reschedules all records associated with that schedule).

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

iRIMS includes two user interfaces for filing records. Using the iRIMS Navigator, users file directly into the iRIMS repository from within the main user interface. They navigate through the file system to select the electronic file, complete the record profile, select a file code, and mark the document "Official" to declare the document as a record.

Users can also use drag and drop functionality to file records. The iRIMS Filing Bin allows users to drag and drop files onto Windows Explorer, complete the record profile, and file the record to iRIMS.

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

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

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

When filing Outlook e-mail that has an attachment(s), iRIMS forces the user to file the e-mail message and the attachment(s) as a single record. If users want to assign different record profile data to attachments, they must first save the attachment to their hard drive and file the record as a regular electronic document. Additionally, users can drag the attached file from the email message to the iRIMS Filing Bin and file the attachment as a regular electronic document.

---

<sup>1</sup> Backwards Compatibility is a new requirement in the June 2002 version of DoD 5015.2-STD.

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

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

File plan and document profile data are stored separately from the actual records in a relational database. MS SQL Server 2000 and Oracle 8.1.7 provided the databases during the compliance tests.

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

Records managers perform screening functions using the Disposition Search template available from the Tools menu. From here, they design queries for information relating to folders or records that are qualified for disposition, including transfer, accession, or destruction. Records managers can enter a future date to calculate disposition for planning purposes.

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

iRIMS offers records managers and privileged users the ability to close folders by assigning edit privileges to folders. Privileged users can only close folders in the record categories to which they have been assigned folder management privileges.

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

To cut off record folders, records managers use the Disposition Search template to search for folders due for Cutoff. A list of folders matching the criteria will display. Records managers select the folder(s) they wish to perform cutoff on and change the Status for the folder(s) to "Cutoff". By cutting off the folder, all records within that folder are cut off as well.

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

iRIMS provides the capability to freeze and unfreeze records at all levels of the file plan. If a record series is frozen, all files, folders, and documents in that series do not qualify for disposition. Once a hold is applied to a record, no more disposition actions can be taken on that record.

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

Records managers define multiple phases within the disposition instructions to distinguish between record transfers and record accessions. In both cases, the records can be removed from the repository, however, records managers can choose to retain the metadata of the transferred records in the system by including an export phase in the disposition schedule. Exporting the records creates a copy of the records for transfer, while allowing records managers to retain the metadata in the RMA until receipt of successful transfer is received.

To search for folders due for accession or transfer, the records manager queries the database using the Disposition Search template. iRIMS presents a list of records that qualify for transfer and the records manager verifies that they should be transferred. iRIMS then writes the affected electronic records and record metadata to a user specified directory and deletes these items from the repository and database. The extracted metadata is in text format.

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

To destroy records, the records manager uses the Disposition Search template to search for records due for destruction, selects them, and verifies that they should be destroyed. iRIMS then deletes the records from the repository and database.

Records cannot be reconstructed once they have been deleted.

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

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

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

iRIMS provides the required capability for searching for and retrieving records. Inter-field operators are available in the event the user wants to perform nested searches. Users with access to the View Customizer can specify what fields should be presented in the search results, and all users can specify the sort order and save frequently used searches. iRIMS allows users to export copies of the records to their hard drives.

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

Records managers assign iRIMS functional access to files, folders and/or documents at the user and/or group level. Permissions are set at the record category or folder level to assign filing and/or search and retrieve access to users/groups.

iRIMS supports multiple-user access. During much of the certification test, two users worked simultaneously performing various functions including filing system maintenance, document filing, record retrieval, reporting, and disposition activities.

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

Administrators determine what events to log for each iRIMS item type by setting auditing interests in the Statistics Maintenance utility available from the Tools menu. Examples of audited events include delete, insert, security classification, and update. iRIMS can also audit user events such as create, update, and delete.

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

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

Operating systems (MS Windows 2000 Server, 2000 Advanced Server) and database management systems (SQL 2000, Oracle 8.1.7) provided the required system management capabilities.

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

### **4.1 *Making Global Changes [C3.2.1.]***

iRIMS provides the capability to make global changes to iRIMS objects. Authorized users can perform batch updates in iRIMS to metadata and/or file categories.

#### **4.2 Bulk Loading Capability [C3.2.2.]**

iRIMS has the capability to bulk load pre-existing file plans. File plans can be loaded using the Import Utility or by using Process Sets, which can combine multiple import files to multiple objects in iRIMS.

iRIMS also has the capability to bulk load electronic records. iRIMS includes a batch electronic record import utility that will import electronic records from a specified directory.

#### **4.3 Interfaces to Other Software Applications [C3.2.3.]**

The iRIMS Filing Bin integrates MS Office applications with iRIMS. Dragging and dropping files onto the Explorer or Outlook Filing Bin(s) will send the record to iRIMS. Additionally, users can import documents into iRIMS from within MS Office applications such as MS Word, by using the "File - Save As" function and selecting the Filing Bin option.

#### **4.4 Bar Code Systems [C3.2.8.]**

iRIMS has the capability to automate circulation activities using bar code technology. Bar codes can be assigned to individual users to facilitate charge in/charge out of iRIMS physical items. In addition, iRIMS has the capability to create, print, and read bar-coded labels. Box transfer tracking and facility space tracking can be used in conjunction with bar coding for records holding facility operations. System administrators can also enable audit tracking of bar coding actions.

#### **4.5 Retrieval Assistance Capability [C3.2.9.]**

iRIMS has advanced searching tools for all main object types, including full text and thesaurus capabilities.

#### **4.6 Print File Label Capability [C3.2.13]**

iRIMS has the capability to create, print, and read bar-coded labels.

### **5. Management of Classified Records**

iRIMS satisfied all Chapter 4 requirements. The following paragraphs highlight iRIMS' implementation of specific Chapter 4 requirements.

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

iRIMS provides the capability to manage classified records using iRIMS security features. When the security features are enabled, users can add metadata that describes the classified record and file it to the iRIMS repository.

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

iRIMS comes with all the classified metadata elements as specified in Table C4.T1. of the Standard.

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

iRIMS provides the capability to establish an automatically triggered classification guide. When a designated classification guide indicator is entered in the "Derived From" field, the "Reason(s) for Classification," "Initial Classification," "Current Classification," and "Declassify On" fields are automatically

populated. Additionally, users will only see those classification guide indicators that match their security profile.

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

Authorized users can search for classified records due for downgrade or declassification. If the classification status of the record changes, authorized users are allowed to edit the classified record metadata.

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

iRIMS provides the capability to handle classified records with the "Restricted Data" and "Formerly Restricted Data" supplemental markings. When a user selects either marking, the "Downgrade On" and "Declassify On" fields are automatically disabled.

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

iRIMS's record history audit captures replaced metadata values, and the user who entered that value. Additionally, iRIMS audit capability has a compare feature, allowing authorized users to bring up a window that shows before and after values for every security classification field.

Users can view, copy, save, and print the audit log based on their access permissions. The capability to delete the audit log is reserved for authorized users only.

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

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

Users are also assigned supplemental markings. Supplemental markings do not override a user's access, but work in conjunction with the user's designated classification level to partition access. Additionally, iRIMS has the ability to restrict access on user-defined fields.

---

Last revision: **30 December 2002**