National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

IBM® DB2® Records Manager V8.4 FP1

Report Number:	CCEVS-VR-VID10222-2009
Dated:	25 February 2009
Version:	1.0

**National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899**

**National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6757
Fort George G. Meade, MD 20755-6757**

ACKNOWLEDGEMENTS

Common Criteria Testing Laboratory

Terrie Diaz, Lead Evaluator
Science Applications International Corporation (SAIC)
Columbia, Maryland

Table of Contents

1 Executive Summary 4
2 Identification 5
3 Organizational Security Policy 6
3.1 Security audit 6
3.2 Identification and authentication 6
3.3 User data protection 7
3.4 Security management 7
3.5 Protection of the TSF 7
4 Assumptions and Clarification of Scope 7
5 Architectural Information 9
6 Documentation 10
7 IT Product Testing 12
7.1 Developer Testing 12
7.2 Evaluation Team Independent Testing 13
7.3 Vulnerability Testing 14
8 Evaluated Configuration 14
9 Results of the Evaluation 18
9.1 Evaluation of the Security Target (ASE) 18
9.2 Evaluation of the Configuration Management Capabilities (ACM) 18
9.3 Evaluation of the Delivery and Operation Documents (ADO) 18
9.4 Evaluation of the Development (ADV) 19
9.5 Evaluation of the Guidance Documents (AGD) 19
9.6 Evaluation of the Life Cycle Support Activities (ALC) 19
9.7 Evaluation of the Test Documentation and the Test Activity (ATE) 19
9.8 Vulnerability Assessment Activity (AVA) 20
9.9 Summary of Evaluation Results 20
10 Validator Comments/Recommendations 20
11 Security Target 20
12 Glossary 20
13 Bibliography 21

1 Executive Summary

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the IBM® Records Manager V8.4.

The Validation Report presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

The evaluation of IBM® Records Manager V8.4 was performed by Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory in the United States and was completed on 10 November 2008.

The information in this report is largely derived from the Security Target (ST), Evaluation Technical Report (ETR) and associated test report. The ST was written by SAIC. The ETR and test report used in developing this validation report were written by SAIC. The evaluation team determined the product to be Part 2 extended and Part 3 conformant, and meets the assurance requirements of EAL 3 augmented with ALC_FLR.2. The product is not conformant with any published Protection Profiles. All security functional requirements are derived from Part 2 of the Common Criteria or expressed in the form of Common Criteria Part 2 requirements.

The TOE is IBM® Records Manager V8.4. Records Manager is a database software application that manages enterprise electronic records and records of physical objects, such as documents and media, throughout their life cycle from creation to disposition.

The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced.

During this validation, the Validators determined that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements defined in the Security Target (ST). Therefore, the Validator concludes that the SAIC findings are accurate, the conclusions justified, and the conformance claims correct.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, commercial testing laboratories, called Common Criteria Testing Laboratories (CCTLs), conduct security evaluations using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 3 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products, desiring a security evaluation, contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- The Protection Profile to which the product is conformant; and
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE:	IBM® Records Manager V8.4
Protection Profile	Not applicable
ST	IBM® Records Manager V8.4 Security Target, Version 1.0, 8 January 2009
Evaluation Technical Report	Evaluation Technical Report For IBM® Records Manager V8.4 (Non-Proprietary), Version 1.0, 21 November 2008, Part 2 (Proprietary), Version 2.0, 23 December 2008
CC Version	Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005

Item	Identifier
Conformance Result	CC Part 2 conformant and Part 3 conformant, EAL 3 augmented with ALC_FLR.2
Sponsor	International Business Machines (IBM)
Developer	International Business Machines (IBM)
Common Criteria Testing Lab (CCTL)	Science Applications International Corporation 7125 Columbia Gateway Drive, Suite 300 Columbia, MD 21046
Evaluation Personnel	Science Applications International Corporation: Terrie Diaz, Dawn Campbell
Validation Body	NIAP CCEVS

3 Organizational Security Policy

This section summarizes the security functions provided by IBM Records Manager that are evident at the various identified network interfaces. It is based on information provided in the Security Target.

3.1 Security audit

The TOE generates audit data and provides an interface, IRM Web Admin, to review audit logs. Audit information generated by the TOE includes date and time of the event, type of event, the identity of the user that caused the event to be generated and the outcome (success or failure) of the event. The TOE restricts the ability to search and review audit data to authorized administrators and provides authorized administrators with the capability to select what auditable events will be audited. The TOE also provides an interface for purging audit records, which is restricted to authorized administrators. The audit records are stored and protected by the underlying database in the IT environment. The IT environment also provides the timestamp for the audit records.

3.2 Identification and authentication

All users of the TOE must have a user account defined in the TOE. The TOE supports two types of users—local and host. A local user is created within the TOE and can log on to the Administrator Web client to perform administrative tasks. A host user is created and exists within the host application. Host users can access the TOE in two ways: from within the host application; and by logging on to the TOE. From the host application, the TOE needs only to know the identity of the host user. It assumes that the host application has already authenticated the user. Host users can also directly log on to the TOE. When logging on, host users must select the host they belong to and use their host user name and password.

The TOE authenticates the user name and password with the host application before allowing the user to log on.

In addition, the host application must be identified and authenticated by the TOE before the host application, or its users, can access TOE services.

The TOE uses AES, implemented in the WebSphere® Application Server (WAS) Java Development Kit (JDK) in the IT environment (in compliance with FIPS140-2, certificate #409), to encrypt user passwords before storing them in the TOE database.

3.3 User data protection

The IRM Engine component enforces an Access Control Security Function Policy (SFP) which restricts access to the file plan components. This protection requires that users of the TOE be authenticated before any access is granted to file plan components. The Access Control SFP can be configured as either an ACL-based policy or as a Role-based policy. The ACL-Based policy uses an Access Control List (ACL) to determine what users and groups can access a file plan component and with what permissions. The Role-based policy also uses ACLs to identify which users and/or groups can access a file plan component, but the access permissions granted to the user are based on defined records management roles that the user is associated with.

Both the ACL-Based and the Role-based policies can also provide additional access controls based on hierarchical security classifications and on non-hierarchical security markings (called security descriptors in the TOE). Note, however, that the TOE does not enforce a full mandatory access control policy. In particular, while a user cannot read a file plan component that has a higher classification than the user’s assigned clearance level, a user with appropriate permissions can create and update file plan components with a lower classification level—the TOE does not prevent “write down” operations.

3.4 Security management

The IRM Web Admin provides authorized administrators the capability to manage the security-related functions and attributes, such as the audit function and management of users and their associated data.

3.5 Protection of the TSF

Records Manager provides the mechanisms to enforce the access control policy ensuring that only authorized users with the appropriate privilege(s) are given access to the resources.

4 Assumptions and Clarification of Scope

The statement of TOE security environment describes the security aspects of the environment in which the TOE is intended to be used and the manner in which it is expected to be deployed. This statement of TOE security environment therefore identifies the assumptions made on the operational environment, the intended method of use for the product, and the organizational security policies with which the product is designed to comply.

Following are the assumptions identified in the Security Target:

- It is assumed Authorized users of the TOE will keep all their authentication data private.
- It is assumed administrative personnel are competent, not careless, willfully negligent, or hostile and will follow and abide by the instructions provided by TOE documentation.
- It is assumed that the IT infrastructure on which the TOE depends is configured in accordance with the manufacturer's installation guides and the evaluated configuration in a secure manner that protects the IT infrastructure and the TOE from any unauthorized users or processes.
- It is assumed the TOE will be located within controlled facilities which will prevent unauthorized physical access and modification.

Following are the threats against the TOE and its environment as identified in the Security Target.

- Authorized users of the TOE may not be held accountable for their actions within the TOE.
- An unauthorized user may gain access to the TOE and its resources in order to bypass, deactivate, or tamper with TOE security functions.
- An unauthorized user may gain access to objects maintained by the TOE in order to modify or destroy them.

Records Manager is dependent on the host application for various services and requires the host application to comply with specific requirements in order to provide an e-records enabled solution. These requirements are described in IBM Records Manager V8.4 Technical Reference Guide (see Section 6.2.4) and are summarized as follows:

- The host application provides the capability for its users to create documents (such as images, e-mail, or spreadsheets) and to modify, view, and retrieve these documents
- The host application provides a suitably secure storage repository to store the documents it generates. (Note that the TOE doesn’t generate, process, or store documents—it manages records of documents or other physical objects or assets.)
- The host application has extensibility capability that allows it and its user interface to be extended or modified in order to integrate with the TOE
- The host application supports J2EE (since the TOE API is based on J2EE technology).

5 Architectural Information[1]

The Records Manager consists of the following components:

- **IRM Engine**—the Engine is a Java 2 Enterprise Edition (J2EE) application that runs on a WebSphere® Application Server. The Engine employs Enterprise Java Beans (EJB) technology. The Engine provides all of the business logic required to enable life cycle management. It implements and manages the official corporate file plan, including the management of retention and disposition rules and related record keeping processes.
- **IRM Administrator Web client**—the Records Manager Administrator Web client is a Web-based administrative user interface that uses the Records Manager Application Programming Interface (API). It is a customizable and extensible J2EE Web-based application that is accessible through a supported browser. It provides the functions for the Records administrators to design, build, and maintain a corporate file plan, and conduct daily records administration activities. A records administrator can use the Records Manager Administrator Web client to perform the following tasks:
    - Design a file plan
    - Define the corporate retention rules
    - Fill the file plan with corporate information
    - Assign the retention rules to the various components of the file plan
    - Import or define users and groups
    - Enforce security by assigning permissions and function access rights
    - Perform periodic retention management activities
    - Create reports
    - Configure audit trails
    - Perform life cycle operations over the Internet, or an Intranet
    - Assign and maintain document security levels.
- **Records Manager Database—**the Records Manager database structure is incorporated within the external repository database. All records reside in the repository to ensure that end users continue to have access to them. The Records Manager database is a DB2 or Oracle database which stores the corporate file plan data, schema, and stored procedures for use with the Records Manager Engine. Note: A Records Manager database must be created before Records Manager can be used; however, the underlying database is part of the TOE environment. The actual documents are stored in the IT environment repository.
- **API**—the API exposes Classes and Methods to enable Records Manager to be integrated with any application and to provide access to the Records Manager server components for the application. The API supports communication through the use of EJBs and can be called from most programming environments. All Engine functions are accessible through the API. Organizations use the API so that

[1] Extracted from SAIC Final ETR Part 1 Version 2.0, 18 November 2008

their e-mail, document management, workflow, imaging, groupware, or other applications will be able to access the Engine to obtain electronic record keeping capability. End users of these products see their participation in record keeping as a feature of the business application they currently use. They do not perform record keeping that is independent of their typical tasks.

- **Import Export Utility**—the Import Export utility provides functionality for importing file plan data to, or exporting file plan data from XML files. For example, this utility can be used to export data items from one Records Manager database to XML files, and then import them to another Records Manager database which is part of another deployment Record Manager.

The following diagram depicts the components of Records Manager as described above in the operating environment.

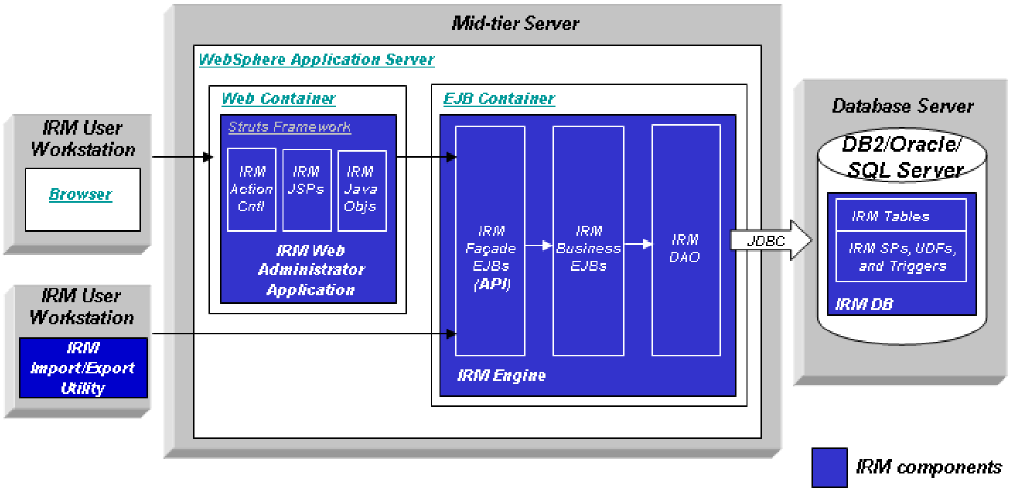

Figure 1: IBM Records Manager architecture

Some development effort is required in order to enable a host application to make use of the services provided by Records Manager. The host application accesses Records Manager through the API, but there are circumstances in which Records Manager must also access the host application. In order to support this access, the host application must implement a Host Connector application that includes two J2EE interfaces published by Records Manager: the HostServiceInterface; and the HostInterface. Once these interfaces are implemented, the host application is registered with Records Manager. This provides a means for Records Manager to uniquely identify and authenticate the host application before it can access Records Manager services.

6 Documentation

Following is a list of the evaluation evidence, each of which was issued by the developer (and sponsor).

Design documentation

Document	Version	Date
IBM Records Manager Version 8.4 Security High-level Functional Specification and Design	Issue 1.5	11 November 2008
RM 84_DesignDocMapping_V.6.xls		

Guidance documentation

Document	Version	Date
IBM Records Manager System Administration Guide Version 8 Release 4		
Addendum to the IBM Records Manager System Administration Guide	Version 1.7	

Configuration Management documentation

Document	Version	Date
IBM Records Manager v8.4 Configuration Management	Issue 0.9	29 September 2008
IBM Records Manager Submitted documentation list		8 October 2008

Delivery and Operation documentation

Document	Version	Date
IBM Records Manager V8.4 Delivery Operation and Guidance	Issue 0.5	16 January 2008
IBM Records Manager Planning and Installing Your Record Management System Version 8 Release 4		
DSW Secure Media Delivery (SMD)	v1.2	
Download Director Command Line Client (DDP) User Guide	Version 3.01	Aug 16, 2004
Tequila for eSD and Golden Master File Transfer to Dublin Release Lab No. SDF-OTH-71	Rev 7	05/02/2007

Life Cycle Support documentation

Document	Version	Date
IBM Records Manager V8.4 Lifecycle document	Issue 0.6	18 January 2008
Records to support alternative to on-site audit		

Test documentation

Document	Version	Date
IBM Records Manager v8.4 Security Related Test Plan	Issue 1.2b	21 November 2008
IBM Records Manager v8.4 Security Related Test Cases	Issue 1.2b	21 November 2008

The actual test results have been submitted to the evaluation team in various wave and video files.

Vulnerability Assessment documentation

Document	Version	Date
IBM Records Manager Version 8.4 Vulnerability Analysis	Issue 1.0	18 November 2008

Security Target

Document	Version	Date
IBM® Records Manager V8.4 Security Target	Version 1.0	8 January 2009

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team.

7.1 Developer Testing

The developer tested the interfaces identified in the functional specification and mapped each test to the security function tested. The scope of the developer tests included all the TSFI. The testing covered the security functional requirements in the ST including: Security audit, User data protection, Identification and authentication, Security management, and Protection of the TSF. All security functions were tested and the TOE behaved as expected. The evaluation team determined that the developer’s actual test results matched the vendor’s expected results.

7.2 Evaluation Team Independent Testing

The evaluation team ran a sample of the automated test suite and a subset of the of the vendor's manual tests. In addition to re-running the vendor's tests, the evaluation team developed a set of independent team tests to address areas of the ST that did not seem completely addressed by the vendor's test suite, or areas where the ST did not seem completely clear. All were run as manual tests.

The vendor provided the TOE software and the necessary computers, hubs, and cabling for the test environment.

The following hardware is necessary to create the test configuration:

- TOE Hardware
    - For Windows - IBM PC, Intel Pentium 4 3.0 GHz, CD-ROM reader (for installation), 40GB Hard Disk, 2GB memory, and network adapter card.
    - For AIX - RS Power 4+ or 5 processor, CD-ROM reader (for installation), 40GB Hard Disk, 4GB memory, and network adapter card.
- IT Environment Hardware
    - For IRM Web Admin - IBM PC, Intel Pentium 4 3.0 GHz, CD-ROM reader (for installation), 40GB Hard Disk, 2GB memory, SVGA display (800 x 600 resolution and 256 color mode), and network adapter card.
- Test Hardware
    - No specific test hardware is required
        - Ethernet router, CAT 5e cabling, and any other items required to create a functional Ethernet network environment
- Test Hardware
    - No specific test hardware is required
- Ethernet router, CAT 5e cabling, and any other items required to create a functional Ethernet network environment.

The following software is required to be installed on the machines used for the test:

TOE	Operating System	Application Server	Database Server Software
Records Manager 8.4	AIX 5.3	WAS 6.1.0.11	DB2 v9.1 FP4
Records Manager 8.4	Windows 2003 SP2	WAS 6.1.0.11	Oracle 10.2.0.3

The following software is required to be installed on the client machines used for the test:

TOE	Operating System
Records Manager Client for Windows 8.4	Windows 2003 SP2

In addition to developer testing, the evaluation team conducted its own suite of tests, which were developed independently of the sponsor. These also completed successfully.

7.3 Vulnerability Testing

The evaluators developed vulnerability tests to address the Protection of the TSF security function, as well as expanding upon the public search for vulnerabilities provided to the team by the sponsor. These tests identified no vulnerabilities in the specific functions provided by the TOE.

8 Evaluated Configuration

The TOE operates in the context of the supporting application server and operating system and utilizes the functions offered by its IT environment to ensure a secure domain for the execution of the TOE, the timestamp for the audit records and password expiration, to protect the TSF data such as the audit records, and to communicate between the components of the TOE. The underlying database is used to store the metadata about records managed by the TOE. The IRM Web Admin is accessed via a web browser through either an HTTP or SSL connection. Communications between the WebSphere® Application Server hosting the IRM Engine and the RDBMS hosting the IRM database (DB2 or Oracle) can be configured to provide encrypted data transmission. This capability is solely within the IT environment. Beyond these specific mechanisms, it is assumed that the IT environment can protect the data transmission and communication between the TOE components as deemed necessary.

The TOE is a database software application that is comprised of the applications required for the correct enforcement of the security functions. The TOE is deployed with single instances of each component and with a single database installed on a separate machine. The API is installed on the same machine as the IRM Engine.

The TOE is dependent on the following hardware and software being in the environment in which it operates.

	Operating System	Software	Hardware
IRM Engine			
AIX	AIX® 5L™ 5.2 (*64-bit*) (Maintenance level 9) AIX 5L 5.3 (*64-bit*) (Maintenance level 5)	IBM DB2 Universal Database 9.1 Fix Pack 4 plus special build (*64-bit*) **ftp://ftp.software.ibm.com/ps/products/db2/fixes2/english-us/special_builds/v9/fp4/** Oracle 10g R2 Database Enterprise Edition (*64-bit*) patchset 3 (Windows) or patch 4722328 (UNIX) **The IBM Records Manager Engine Configuration tool uses JCC type 4 JDBC drivers to connect to remote DB2 databases:** Oracle 10g R2 Client 10.2.0.3 with patchset 3 (Windows [patch 5916257]) or patch 4722328 (AIX) WebSphere® Application Server 6.1 Fix Pack 11 or later (*32-bit*)	**Minimum Requirements:** **Processor:** Engine and database on same server: Dual 1.0 GHz Engine and database on different servers (each server): pSeries 1.0 GHz **RAM:** 4.0 GB or greater **Hard driver:** 40.0 GB (Depends on storage requirements including file plan size and number of records) **Need a CD-ROM Drive**

		WebSphere® Application Server Network Deployment Edition 6.1 Fix Pack 11 or later *(32-bit)*	
Windows	Microsoft® Windows Server 2003 Standard Edition *(32-bit)* or with SP1 Microsoft Windows Server 2003 Standard Edition SP2 *(32-bit)* Microsoft Windows Server 2003 Enterprise Edition *(32-bit)* or with SP1 Microsoft Windows Server 2003 Enterprise Edition SP2 *(32-bit)* Microsoft Windows Server 2003 R2 *(32-bit)* Microsoft Windows Server 2003 R2 SP2 *(32-bit)*	IBM DB2 Universal Database 9.1 Fix Pack 4 plus special build (*32-bit*) **ftp://ftp.software.ibm.com/ps/products/db2/fixes2/english-us/special_builds/v9/fp4/** Oracle 10g R2 Database Enterprise Edition (*32-bit*) patchset 3 (Windows) or patch 4722328 (UNIX) Oracle 10g R2 Database Enterprise Edition (*64-bit*) patchset 3 (Windows) or patch 4722328 (UNIX) **The IBM Records Manager Engine Configuration tool uses JCC type 4 JDBC drivers to connect to remote DB2 databases:** Oracle 10g R2 Client 10.2.0.3 with patchset 3 (Windows [patch 5916257]) or patch 4722328 (AIX) WebSphere® Application Server 6.1 Fix Pack 11 or later (*32-bit*) WebSphere® Application Server Network Deployment Edition 6.1 Fix Pack 11 or later *(32-bit)*	**Minimum Requirements:** **Processor:** Engine and database on same server: Dual 1.0 GHz Engine and database on different servers (each server): pSeries 1.0 GHz **RAM:** 4.0 GB or greater **Hard driver:** 40.0 GB (Depends on storage requirements including file plan size and number of records) **Need a CD-ROM Drive**
IRM Database			
AIX	AIX® 5L™ 5.2 (*64-bit*) (Maintenance level 9) AIX 5L 5.3 (*64-bit*) (Maintenance level 5)	IBM DB2 Universal Database 9.1 Fix Pack 4 plus special build (*64-bit*) **ftp://ftp.software.ibm.com/ps/products/db2/fixes2/english-us/special_builds/v9/fp4/** Oracle 10g R2 Database Enterprise Edition (*64-bit*) patchset 3 (Windows) or patch 4722328 (UNIX) **The IBM Records Manager Engine Configuration tool uses JCC type 4 JDBC drivers to connect to remote DB2 databases:** Oracle 10g R2 Client 10.2.0.3 with patchset 3 (Windows [patch 5916257]) or patch 4722328 (AIX) WebSphere® Application Server 6.1 Fix Pack 11 or later (*32-bit*) WebSphere® Application Server Network Deployment Edition 6.1 Fix Pack 11 or later *(32-bit)*	**Minimum Requirements:** **Processor:** Engine and database on same server: Dual 1.0 GHz Engine and database on different servers (each server): pSeries 1.0 GHz **RAM:** 4.0 GB or greater **Hard driver:** 40.0 GB (Depends on storage requirements including file plan size and number of records) **Need a CD-ROM Drive**
Windows	Microsoft® Windows Server 2003 Standard Edition *(32-bit)* or with SP1	IBM DB2 Universal Database 9.1 Fix Pack 4 plus special build (*32-bit*) **ftp://ftp.software.ibm.com/ps/products/db2/fixes2/english-us/special_builds/v9/fp4/**	**Minimum Requirements:** **Processor:** Engine and database on same server: Dual 1.0 GHz

	Microsoft Windows Server 2003 Standard Edition SP2 *(32-bit)* Microsoft Windows Server 2003 Enterprise Edition *(32-bit)* or with SP1 Microsoft Windows Server 2003 Enterprise Edition SP2 *(32-bit)* Microsoft Windows Server 2003 R2 *(32-bit)* Microsoft Windows Server 2003 R2 SP2 *(32-bit)*	Oracle 10g R2 Database Enterprise Edition (*32-bit*) patchset 3 (Windows) or patch 4722328 (UNIX) Oracle 10g R2 Database Enterprise Edition (*64-bit*) patchset 3 (Windows) or patch 4722328 (UNIX) **The IBM Records Manager Engine Configuration tool uses JCC type 4 JDBC drivers to connect to remote DB2 databases:** Oracle 10g R2 Client 10.2.0.3 with patchset 3 (Windows [patch 5916257]) or patch 4722328 (AIX) WebSphere® Application Server 6.1 Fix Pack 11 or later (*32-bit*) WebSphere® Application Server Network Deployment Edition 6.1 Fix Pack 11 or later *(32-bit)*	Engine and database on different servers (each server): pSeries 1.0 GHz **RAM:** 4.0 GB or greater **Hard driver:** 40.0 GB (Depends on storage requirements including file plan size and number of records) **Need a CD-ROM Drive**
Import/Export Utility			
AIX	AIX 5L 5.2 (*64-bit*) (Maintenance level 9) AIX 5L 5.3 (*64-bit*) (Maintenance level 5)	WebSphere® Application Server 6.1.0.11 J2EE Client Runtime *(32-bit)* WebSphere® Application Server 6.1.0.11 J2EE Client Runtime *(64-bit)*	**No particular requirement**
Windows	Microsoft® Windows Server 2003 Standard Edition *(32-bit)* or with SP1 Microsoft Windows Server 2003 Standard Edition SP2 *(32-bit)* Microsoft Windows Server 2003 Enterprise Edition *(32-bit)* or with SP1 Microsoft Windows Server 2003 Enterprise Edition SP2 *(32-bit)* Microsoft Windows Vista™ Microsoft Windows XP Professional SP2 Microsoft Windows Server	WebSphere® Application Server 6.1.0.11 J2EE Client Runtime *(32-bit)* WebSphere® Application Server 6.1.0.11 J2EE Client Runtime *(64-bit)* Microsoft Internet Explorer 6 SP1 or later Microsoft Internet Explorer 7.x	**Minimum Requirement:** Processor: Intel Pentium III™ or AMD® equivalent Memory: 256 MB Free disk space: 2 GB

	2003 R2 *(32-bit)* Microsoft Windows Server 2003 R2 SP2 *(32-bit)*		
IRM Web Admin			
AIX	AIX 5L 5.2 (*64-bit*) (Maintenance level 9) AIX 5L 5.3 (*64-bit*) (Maintenance level 5)	WebSphere® Application Server 6.1.0.11 J2EE Client Runtime *(32-bit)* WebSphere® Application Server 6.1.0.11 J2EE Client Runtime *(64-bit)*	**No particular requirement**
Windows	Microsoft® Windows Server 2003 Standard Edition *(32-bit)* or with SP1 Microsoft Windows Server 2003 Standard Edition SP2 *(32-bit)* Microsoft Windows Server 2003 Enterprise Edition *(32-bit)* or with SP1 Microsoft Windows Server 2003 Enterprise Edition SP2 *(32-bit)* Microsoft Windows Vista™ Microsoft Windows XP Professional SP2 Microsoft Windows Server 2003 R2 *(32-bit)* Microsoft Windows Server 2003 R2 SP2 *(32-bit)*	WebSphere® Application Server 6.1.0.11 J2EE Client Runtime *(32-bit)* WebSphere® Application Server 6.1.0.11 J2EE Client Runtime *(64-bit)* Microsoft Internet Explorer 6 SP1 or later Microsoft Internet Explorer 7.x	**Minimum Requirement:** Processor: Intel Pentium III™ or AMD® equivalent Memory: 256 MB Free disk space: 2 GB

Note that the minimum hardware requirements for the IRM Engine and IRM Database assume these are installed on separate servers. These two components can be installed on a single server, but this requires a higher performance processor. Full details are provided in *IBM Records Manager Version 8.4 Planning and Installing Guide*.

9 Results of the Evaluation

The evaluation was conducted based upon the Common Criteria (CC), Version 2.3, dated August 2005; the Common Evaluation Methodology (CEM), Version 2.3, dated August 2005; and all applicable International Interpretations in effect on March 2007. The evaluation confirmed that the IBM® Records Manager V8.4 product is compliant with the Common Criteria Version 2.3, functional requirements (Part 2), Part 2 conformant, and assurance requirements (Part 3) for EAL3 Augmented with ALC_FLR.2. The details of the evaluation are recorded in the CCTL's evaluation technical report; Evaluation Technical Report for IBM® Records Manager V8.4, Part 1 (Non-Proprietary) and Part 2 (Proprietary). The product was evaluated and tested against the claims presented in the IBM® Records Manager V8.4 Security Target, Version 1.0, 8 January 2009.

The Validators followed the procedures outlined in the Common Criteria Evaluation Scheme publication number 3 for Technical Oversight and Validation Procedures. The Validators observed that the evaluation and all of its activities were in accordance with the Common Criteria, the Common Evaluation Methodology, and the CCEVS. The Validators therefore conclude that the evaluation team's results are correct and complete.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of threats, policies, and assumptions, a statement of security requirements claimed to be met by the IBM® DB2® Records Manager V8.4 product that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

9.2 Evaluation of the Configuration Management Capabilities (ACM)

The evaluation team applied each EAL 3 augmented with ALC_FLR.2 ACM CEM work unit. The ACM evaluation ensured the TOE is identified such that the consumer is able to identify the evaluated TOE. The evaluation team ensured the adequacy of the procedures used by the developer to accept, control, and track changes made to the TOE implementation, design documentation, test documentation, user and administrator guidance, security flaws and the CM documentation. The evaluation team ensured the procedure included automated support to control and track changes to the implementation representation. The procedures reduce the risk that security flaws exist in the TOE implementation or TOE documentation. To support the ACM evaluation, the evaluation team received Configuration Management (CM) records from IBM.

9.3 Evaluation of the Delivery and Operation Documents (ADO)

The evaluation team applied each EAL 3 augmented with ALC_FLR.2 ADO CEM work unit. The ADO evaluation ensured the adequacy of the procedures to deliver, install, and configure the TOE securely. The evaluation team ensured the procedures addressed the detection of modification, the discrepancy between the developer master copy and the version received, and the detection of attempts to masquerade as the developer.

The evaluation team followed the IBM DB2 Records Manager Version 8 Release 4 Planning and Installing Your Document Management System to test the installation procedures to ensure the procedures result in the evaluated configuration.

9.4 Evaluation of the Development (ADV)

The evaluation team applied each EAL 3 augmented with ALC_FLR.2 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification and a high-level design document. The evaluation team also ensured that the correspondence analysis between the design abstractions correctly demonstrated that the lower abstraction was a correct and complete representation of the higher abstraction.

9.5 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each EAL 3 augmented with ALC_FLR.2 AGD CEM work unit. The evaluation team ensured the adequacy of the guidance documents in describing how to securely administer the TOE. The IBM DB2 Records Manager Version 8 Release 4 Planning and Installing Your Document Management System and the IBM DB2 Records Manager System Administration Guide Version 8 Release 4 were assessed during the design and testing phases of the evaluation to ensure it was complete.

9.6 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each EAL 3 augmented with ALC_FLR.2 ALC CEM work unit. The evaluation team ensured the adequacy of the developer procedures to protect the TOE and the TOE documentation during TOE development and maintenance to reduce the risk of the introduction of TOE exploitable vulnerabilities during TOE development and maintenance. To support the ALC evaluation, the Vendor submitted videos and electronic records in lieu of an onsite audit. The evidence submitted, demonstrated the use of the security measures as described in the Life Cycle documentation and sampled records created by using the security procedures.

In addition to the EAL 3 ALC CEM work units, the evaluation team applied the ALC_FLR.2 work units from the CEM supplement. The flaw remediation procedures were evaluated to ensure that systematic procedures exist for managing flaws discovered in the TOE.

9.7 Evaluation of the Test Documentation and the Test Activity (ATE)

The Evaluation Team applied each EAL 3 augmented with ALC_FLR.2 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. Specifically, the evaluation team ensured that the vendor test documentation sufficiently addresses the security functions as described in the functional specification and high-level design specification. The evaluation team exercised the complete Vendor test suite and devised an independent set of team test and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

9.8 Vulnerability Assessment Activity (AVA)

The Evaluation Team applied each EAL 3 augmented with ALC_FLR.2 AVA CEM work unit. The evaluation team ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the developer vulnerability analysis, the evaluation team's misuse analysis, the evaluation team's vulnerability analysis, and the evaluation team's performance of penetration tests.

9.9 Summary of Evaluation Results

The Evaluation Team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the Evaluation Team's performance of the entire set of the vendor's test suite, the independent tests, and the penetration test also demonstrated the accuracy of the claims in the ST.

10 Validator Comments/Recommendations

The validation team observed that the evaluation was performed in accordance with the CC, the CEM, and CCEVS practices. The Validation team agrees that the CCTL presented appropriate rationales to support the Results presented in Section 5 of the ETR and the Conclusions presented in Section 6 of the ETR.

The validation team, therefore, recommends that the evaluation and Pass result for the identified TOE be accepted.

11 Security Target

The Security Target is identified as IBM® Records Manager V8.4 Security Target, Version 1.0, dated 08 January 2009. The document identifies the security functional requirements (SFRs) necessary to implement the TOE security policies. These include TOE SFRs and IT Environment SFRs. Additionally, the Security Target specifies the security assurance requirements necessary for EAL 3 augmented with ALC_FLR.2.

12 Glossary

The following definitions are used throughout this document:

AIX	Advanced Interactive eXecutive (a UNIX-style operating system)
API	Application Programming Interface
CC	Common Criteria
CEM	Common Evaluation Methodology

CCEVS	Common Criteria Evaluation and Validation Scheme
DAO	Data Access Objects
UDB	Universal Database
DoD	Department of Defense
EAL	Evaluation Assurance Level
EJB	Enterprise Java Beans
GUI	Graphical User Interface
HLD	High-level Design
HTTP	HyperText Transfer Protocol
IA	Initial Assessment
IIOP/RMI	Internet Inter-Orb Protocol/ Remote Method Invocation
IRM	IBM Records Manager
J2EE	Java2 Enterprise Edition
JSP	Java Server Pages
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
PP	Protection Profile
RDBMS	Relational Data Base Management System
SAIC	Science Applications International Corporation
SOAP	Simple Object Access Protocol
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
US	United States
WAS	WebSphere® Application Server

13 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, Version 2.3, August 2005.

[2] Common Criteria for Information Technology Security Evaluation - Part 2: Security Functional Requirements, Version 2.3, August 2005.

[3] Common Criteria for Information Technology Security Evaluation - Part 3: Security Assurance Requirements, Version 2.3, August 2005.

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 2.3, August 2005.

[5] IBM® Records Manager V8.4 Final ETR – Part 2 (Proprietary), Version 2.0 dated 23 December 2008 and Supplemental Team Test Report, Version 1.0, 21 November 2008.

[6] IBM® Records Manager V8.4 Final ETR – Part 1 (Non-Proprietary), Version 1.0, 21 November 2008.

[7] IBM® Records Manager V8.4 Security Target, Version 1.0, 8 January 2009.

[8] NIAP Common Criteria Evaluation and Validation Scheme for IT Security, Guidance to Common Criteria Testing Laboratories, Version 1.0, March 20, 2001.