IBM® Records Manager V8.4
Security Target

ST Version 1.0

8 January 2009

Prepared for:
International Business Machines (IBM)
555 Bailey Avenue
San Jose, CA 95161

Prepared By:
Science Applications International Corporation
Common Criteria Testing Laboratory
7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046

TABLE OF CONTENTS

LIST OF TABLES

1. Security Target Introduction

This section provides the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE is the IBM® Records Manager V8.4 product provided by International Business Machines (IBM). IBM 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 Security Target contains the following additional sections:

- TOE Description (Section 2): This section gives an overview of the TOE, describes the TOE in terms of its physical and logical boundaries, and states the scope of the TOE.
- Security Environment (Section 3): This section details the threats to be countered by the TOE and assumptions about the intended TOE environment and method of use.
- Security Objectives (Section 4): This section details the security objectives for the TOE and its environment.
- IT Security Requirements (Section 5): This section presents the security functional requirements (SFR) for the TOE and the IT Environment that supports the TOE, and details the security assurance requirements (SARs) for EAL 3 augmented with ALC_FLR.2.
- TOE Summary Specification (Section 6): This section describes the security functions provided by the TOE and the assurance measures that satisfy the security requirements.
- Protection Profile Claims (Section 7): This section identifies any Protection Profile Claims made in the ST.
- Rationale (Section 8): This section documents the justifications of the security objectives, security requirements and TOE summary specification as to their consistency, completeness and suitability.

1.1 Security Target, TOE and CC Identification

ST Title – IBM® Records Manager V8.4 Security Target

ST Version – Version 1.0

ST Date – 8 January 2009

TOE Identification – IBM® Records Manager V8.4

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005.

1.2 Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 2.3, August 2005.
    - Part 2 Conformant
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 2.3, August 2005.
    - Part 3 Conformant
    - EAL 3 augmented with ALC_FLR.2

1.3 Conventions, Terminology, Abbreviations

This section specifies the formatting conventions and defines TOE-specific terminology and abbreviations used within the ST.

1.3.1 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a letter in parenthesis placed at the end of the component. For example FDP_ACC.1a and FDP_ACC.1b indicate that the ST includes two iterations of the FDP_ACC.1 requirement, a and b.
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]).
    - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
    - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.3.2 Terminology

Authorized administrators	The TOE defines a built-in group, "Administrators", and a built-in user, "Administrator", which is a member of the Administrators group. The Administrators group is given all function access rights, which are then inherited by the Administrator user. The authorized administrators of the TOE are users that are assigned to the Administrators group (including Administrator) and users that are granted (directly or via group membership) one or more function access rights that provide access to security management functions. When "authorized administrators" is used within the ST, it should be understood to mean "users with the appropriate function access right for the relevant security management function".
Authorized Users	The users, administrative and non-administrative, who have been given access to the TOE.
Business Infrastructure	The operating framework that includes the network, hardware, and software used in a business's day to day operations.
File Plan	A plan that specifies how records are organized. A file plan helps Records Administrators apply retention policies to records, and to easily retrieve, use, and dispose of records. A file plan is similar to a hard disk drive that is divided into folders and subfolders.
Function access rights	The TOE uses **function access rights** to control access to its features, including security management functions. These are described in further detail in Section 6.
Host Application	An external application that uses the TOE to provide life cycle retention management. The responsibilities of the host application are to generate electronic information, to provide tools to manipulate the data, and to maintain a repository to store the information.

Permissions	Permissions define what an individual user or group can do to a specific file plan component. They determine if a user is allowed to perform a requested operation on a file plan component. Permissions are described in further detail in Section 6.1.2.
Records management role	The TOE can be configured to enforce a role-based access control policy. Under this policy, users are assigned to **records management roles** and permissions to access file plan components are granted based on the user's assigned records management roles. Authorized administrators are able to create, modify and delete records management roles. Records management roles are distinct from the security management roles maintained by the TOE.
Unauthorized Users	Users and processes that have not been granted access to the TOE.
View	A collection of relationships between components that comprise the file plan, similar to the way that a view in a relational database is a collection of joined tables that comprise a schema. File plan views give each component in the file plan a context. No file plan components can exist outside a view. Every file plan component must be in at least one view (Hierarchical, Link, or Set).

1.3.3 Abbreviations

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

2. TOE Description

The Target of Evaluation (TOE) is IBM® Records Manager V8.4, 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. It is henceforth referred to as Records Manager, or IRM.

2.1 TOE Overview

IBM Records Manager (IRM) is an electronic records technology that manages enterprise electronic records and records of physical objects, such as documents and media, throughout their life cycle from creation to disposition. Within the IRM, the two types of records are treated the same. IRM is used to store descriptive metadata about the objects, and track that information within the object's profile. It provides life cycle records retention management for various applications, such as e-mail, document management, workflow, imaging, and groupware. In addition, Records Manager can use IBM® DB2® Content Manager to serve as a document repository, but this is not required in the evaluated configuration[1].

Records Manager does not include a predefined file plan (specifying how records are organized), or a predefined user interface and workflow. This means that administrators of organizations that employ records management procedures are able to use the TOE to design their own custom file plan and determine the users that will have access to the file plan.

The file plan structure comprises file plan components. There are two types of file plan component:

- **Container components**—represent physical or logical record containers, such as files, folders, departments, boxes, or floors in a building
- **Record components**—represent actual records. They differ from container components in that they can have content. Examples of record components are documents, email messages, and illustrations.

The Records administrator creates file plan component definitions, which specify the types of file plan component that will exist in the file plan. Each file plan component in a file plan is an instantiation of a file plan component definition.

All file plan component definitions include a number of built-in attributes, also known as "system" attributes. System attributes define such properties of the file plan component as name, creation date, or custodian. In addition to its system attributes, a file plan component definition can be extended by the definition of custom attributes, which can define properties unique to the file plan component type being defined.

Records administrators use Records Manager to model and create their corporation's file plan, as well as life cycle retention rules. This information is then applied to all records identified in the file plan to determine their effective retention life cycle. The Records administrator configures the file plan, the classification scheme, assigns retention rules, conducts global updates, defines and implements access control, and designs and generates statistical, operational and maintenance reports for audit purposes.

2.2 TOE Architecture

The design of Records Manager technology is for the purpose of interacting seamlessly with applications[2]. It is a component of a larger external business infrastructure which includes applications such as email, document, data storage, and other computer systems and leverages the existing infrastructure of the host application, thereby eliminating redundancy. Records Manager is optimized to provide life cycle retention management for electronic records, while the host application manages document creation, management, storage, and retrieval.

[1] The capability of the TOE to interoperate with IBM® DB2® Content Manager and IBM® DB2® Document Manager is outside the scope of the evaluation.

[2] The TOE guidance documentation refers to this as "embedding". To the user of the host application, the TOE appears to be an extension of the host application. However, the TOE is not physically embedded within the host application.

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 fully 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 using the Records Manager Administrator Web client might perform the following typical 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 various 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 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 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 the another deployment Record Manager.

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

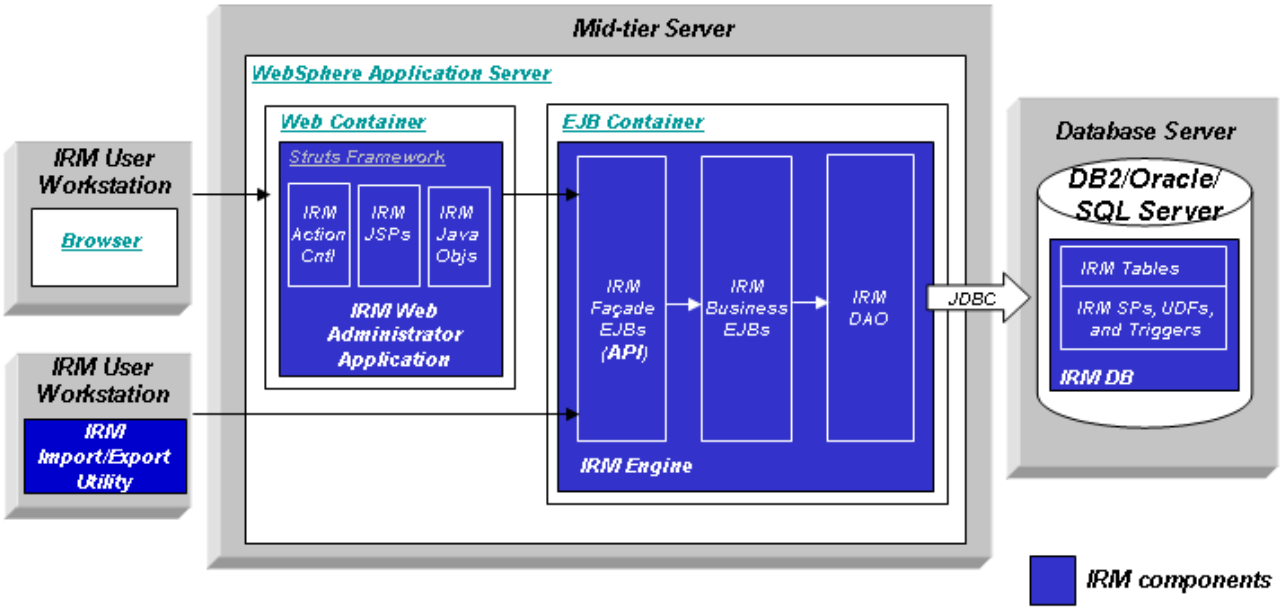

Figure 1: IBM Records Manager architecture

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.

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).

2.2.1 Physical Boundaries

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*) 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 drive:** 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 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*)	**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 drive:** 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)*	
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 drive:** 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 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 drive:** 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 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
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*.

2.2.2 Logical Boundaries

This section identifies the security functions that Records Manager provides. The logical boundaries of the TOE include the security functions of the TOE interfaces. The TOE logically supports security audit, user data protection, identification and authentication, security management and protection of the TSF.

2.2.2.1 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.

2.2.2.2 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.

2.2.2.3 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), to encrypt a user's password before storing it in the TOE database.

2.2.2.4 Security management

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

2.2.2.5 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.

2.2.3 Excluded Functionality

The following features and capabilities described in the guidance documentation for the TOE are excluded from the evaluation:

- Customizable Web Client interface—the guidance documentation describes how a host application vendor can enhance, customize, or re-write an entirely new user interface for Records Manager Administrator. However, the security management capabilities in the evaluated configuration are accessed via the IRM Web Administrator client supplied with the TOE, and any change to this component, or replacement with a different administration client, will take the TOE out of its evaluated configuration
- Support for bar code scanning—the capability to add new file plan components to a file plan by scanning a bar code affixed to the physical record is not covered by the evaluation.

2.3 TOE Documentation

IBM supplies administration and user guidance documents to help ensure that the evaluated Records Manager product can be operated and used securely and can be correctly integrated with host applications in order to ensure that Records Manager provides the expected records management capability. These and other documents are further summarized in section 6.2.

3. Security Environment

The TOE security environment describes the security aspects of the intended environment in which the TOE is to be used and the manner in which it is expected to be employed. The statement of TOE security environment defines the following:

- Threats that the product is designed to counter.
- Assumptions made on the operational environment and the method of use intended for the product.

The TOE provides for a level of protection that is appropriate for IT environments that require control over what information is accessed by the users on the systems. It is suitable for use in both commercial and government environments. Note that while the identified threats are mitigated by security functions implemented in the TOE and/or its supporting IT environment, the overall assurance level (EAL 3 augmented with ALC_FLR.2) also serves as an indicator of whether the TOE would be suitable for a given environment.

3.1 Threats

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

3.2 Assumptions

A.AUTH_DATA	Authorized users of the TOE will keep all their authentication data private.
A.NOEVIL	The administrative personnel are competent, not careless, willfully negligent, or hostile and will follow and abide by the instructions provided by TOE documentation.
A.SECURE_ENV	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.
A.PROTECT	The TOE will be located within controlled facilities which will prevent unauthorized physical access and modification.

4. Security Objectives

This section defines the security objectives of the TOE and its supporting environment. Security objectives, categorized as either IT security objectives or non-IT security objectives, reflect the stated intent to counter identified threats and/or comply with any organizational security policies identified. All of the identified threats and organizational policies are addressed under one of the categories below.

4.1 Security Objectives for the TOE

O.AUDIT	The TSF must provide the means to record and review an audit trail of security related events such that users can be held accountable for their security relevant actions.
O.AUTHORIZE	The TOE must ensure that only authorized users and administrators gain access to the TOE and its resources.
O.AUTH_DATA	The TOE must allow authorized users to modify their own authentication data.
O.MANAGE	The TOE must allow administrators to effectively manage the TOE, and its security functions, and must ensure that only authorized administrators are able to access its functionality.
O.OBJ_ACCESS	The TOE must limit access to objects maintained by the TOE to users with authorization and appropriate privileges. The TSF must allow authorized users to specify which users may access their objects and the actions performed on the objects.
O.SELPRO	The TOE must protect itself against attempts by unauthorized users to bypass or deactivate TOE security functions.

4.2 Security Objectives for the IT Environment

OE.SEP	The TOE operating environment shall provide mechanisms to isolate the TSF and assure that TSF components cannot be tampered with or bypassed.
OE.TIME	The IT environment shall provide an accurate timestamp.
OE.TRANSFER	The IT environment shall ensure the data transmitted between TOE components and between the TOE and non-TOE components is protected from tampering and disclosure.
OE.HOST_AUTH	The host application shall authenticate each user that it defines before allowing any other host-mediated actions on behalf of that user.

4.3 Security Objectives for the Environment

OE.ADMIN	The administrative personnel are competent, not careless, willfully negligent, or hostile and will follow and abide by the instructions provided by TOE documentation.

OE.AUTH_DATA	Those responsible for the TOE must ensure that all access credentials, such as passwords, are protected by the users in a manner that maintains IT security objectives.
OE.INSTALL	Those responsible for the TOE must ensure that the TOE and its operating environment is delivered, installed, managed, and operated in a manner that is consistent with the TOE security objectives.
OE.PHYS	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.

5. IT Security Requirements

This section specifies the security functional requirements and security assurance requirements for the TOE, as well as necessary security functional requirements for the IT environment of the TOE.

5.1 TOE Security Functional Requirements

The following table identifies the Security Functional Requirements (SFRs) that are satisfied by IBM Records Manager V8.4.

Requirement Class	Requirement Component
FAU: Security audit	FAU_GEN.1: Audit data generation
	FAU_GEN.2: User identity association
	FAU_SAR.1: Audit review
	FAU_SAR.2: Restricted audit review
	FAU_SAR.3 : Selectable audit review
	FAU_SEL.1 : Selective audit
	FAU_STG.1a : Protected audit trail storage
FDP: User data protection	FDP_ACC.2a: Complete access control
	FDP_ACC.2b: Complete access control
	FDP_ACF.1a: Security attribute based access control
	FDP_ACF.1b: Security attribute based access control
FIA: Identification and authentication	FIA_ATD.1a: User attribute definition
	FIA_ATD.1b: User attribute definition
	FIA_ATD.1c: User attribute definition
	FIA_UAU.2a: User authentication before any action
	FIA_UID.2: User identification before any action
FMT: Security management	FMT_MOF.1: Management of security functions behavior
	FMT_MSA.1a: Management of security attributes
	FMT_MSA.1b: Management of security attributes
	FMT_MSA.1c: Management of security attributes
	FMT_MSA.1d: Management of security attributes
	FMT_MSA.1e: Management of security attributes
	FMT_MSA.1f: Management of security attributes
	FMT_MSA.1g: Management of security attributes
	FMT_MSA.1h: Management of security attributes
	FMT_MSA.1i: Management of security attributes
	FMT_MSA.1j: Management of security attributes
	FMT_MSA.3a: Static attribute initialization
	FMT_MSA.3b: Static attribute initialization
	FMT_MTD.1a: Management of TSF data
	FMT_MTD.1b: Management of TSF data
	FMT_MTD.1c: Management of TSF data
	FMT_MTD.1d: Management of TSF data
	FMT_MTD.1e: Management of TSF data
	FMT_MTD.1f: Management of TSF data
	FMT_MTD.1g: Management of TSF data
	FMT_SAE.1: Time-limited authorization
	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.1: Security roles
FPT: Protection of the TSF	FPT_RVM.1: Non-bypassability of the TSP

Table 1 TOE Security Functional Components

5.1.1 Security audit (FAU)

5.1.1.1 Audit data generation (FAU_GEN.1)

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events: a) Start-up and shutdown of the audit functions; b) All auditable events for the **[*not specified*]** level of audit; and c) **[Authentication attempts and successful administrative actions]**.

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **[no additional information]**.

5.1.1.2 User identity association (FAU_GEN.2)

FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

5.1.1.3 Audit review (FAU_SAR.1)

FAU_SAR.1.1 The TSF shall provide **[Administrator, Users with Audit Management and Audit Reporting Function Access Rights]** with the capability to read **[all audit information]** from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.1.1.4 Restricted audit review (FAU_SAR.2)

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

5.1.1.5 Selectable audit review (FAU_SAR.3)

FAU_SAR.3.1 The TSF shall provide the ability to perform **[*searches, sorting*]** of audit data based on **[user identity, event type]**.

5.1.1.6 Selective audit (FAU_SEL.1)

FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:
a) **[*event type*]**
b) **[no additional attributes]**

5.1.1.7 Protected audit trail storage (FAU_STG.1a)

FAU_STG.1a.1 The TSF shall protect the stored audit records from unauthorised deletion.

FAU_STG.1a.2 The TSF shall be able to **[*prevent*]** unauthorised modifications to the stored audit records in the audit trail.

5.1.2 User data protection (FDP)

5.1.2.1 Complete access control (FDP_ACC.2a – ACL-Based Access Control)

FDP_ACC.2a.1 The TSF**, when configured for ACL-Based Access Control,** shall enforce the **[ACL-Based Access Control SFP]** on **[**
Subjects: Users
Objects: File Plan Components]
and all operations among subjects and objects covered by the SFP.

FDP_ACC.2a.2 The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.

5.1.2.2 Complete access control (FDP_ACC.2b – Role-Based Access Control)

FDP_ACC.2b.1 The TSF**, when configured for Role-Based Access Control,** shall enforce the **[Role-Based Access Control SFP]** on **[**
Subjects: Users
Objects: File Plan Components]
and all operations among subjects and objects covered by the SFP.

FDP_ACC.2b.2 The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.

5.1.2.3 Security attribute based access control (FDP_ACF.1a – ACL-Based Access Control)

FDP_ACF.1a.1 The TSF shall enforce the **[ACL-Based Access Control SFP]** to objects based on the following: **[**
Users:

- **Identity**
- **Groups**
- **Security Descriptors**
- **Security Classification**
- **Function Access Rights**

File Plan Components:

- **Access Control List**
- **Security Descriptors**
- **Security Classification**
- **Custodian**
- **Field Level Permissions]**

FDP_ACF.1a.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[**

The requested operation is allowed if:

- **The User or a Group of which the User is a member has the File Plan Administration Function Access Right, and**
- **(The Access Control List grants the appropriate permission to the User Identity or to a Group the User is a member of) or (the File Plan Component Custodian is the User Identity or is a Group of which the User is a member), and**
- **The File Plan Component Security Classification is not greater than the User Security Classification, and**
- **(Security descriptor control access level is not set to Strict) or (Security descriptor control access level is set to Strict and the File Plan Component Security Descriptors are a subset of the union of the User Security Descriptors and the Security Descriptors of all Groups the User is a member of).**

If all the above checks pass and the requested operation is allowed on the File Plan Component, then if Field Level Permissions are set for individual fields of the File Plan Component, the following checks are made for each field that has permissions set to determine if the requested operation can be performed on the field:

- **If the requested operation is Add then the Field Level Permission must grant Add to the User Identity or to a Group of which the User is a member**
- **If the requested operation is Update then the Field Level Permission must grant Update to the User Identity or to a Group of which the User is a member]**.

FDP_ACF.1a.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **[the User is a member of the Administrators Group]**.

FDP_ACF.1a.4 The TSF shall explicitly deny access of subjects to objects based on the **[no additional rules]**.

5.1.2.4 Security attribute based access control (FDP_ACF.1b – Role-Based Access Control)

FDP_ACF.1b.1 The TSF shall enforce the **[Role-Based Access Control SFP]** to objects based on the following: **[**
Users:

- **Identity**
- **Groups**
- **Records Management Roles**
- **Security Descriptors**
- **Security Classification**
- **Function Access Rights**

File Plan Components:

- **Access Control List**
- **Role Permissions**
- **Security Descriptors**
- **Security Classification**
- **Custodian**
- **Field Level Permissions]**

FDP_ACF.1b.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[**

The requested operation is allowed if:

- **The User or a Group of which the User is a member or one of the User's Records Management Roles has the File Plan Administration Function Access Right, and**
- **(The Access Control List includes the User Identity or a Group the User is a member of and the Role Permissions grant the appropriate permission to a Records Management Role to which the User is allocated) or (the File Plan Component Custodian is the User Identity or is a Group of which the User is a member), and**
- **The File Plan Component Security Classification is not greater than the User Security Classification, and**
- **(Security descriptor control access level is not set to Strict) or (Security descriptor control access level is set to Strict and the File Plan Component Security Descriptors are a subset of the union of the User Security Descriptors and the Security Descriptors of all Groups and Records Management Roles the User is a member of).**

If all the above checks pass and the requested operation is allowed on the File Plan Component, then if Field Level Permissions are set for individual fields of the File Plan Component, the following checks are made for each field that has permissions set to determine if the requested operation can be performed on the field

- **If the requested operation is Add then the Field Level Permission must grant Add to the User Identity or to a Group of which the User is a member**
- **If the requested operation is Update then the Field Level Permission must grant Update to the User Identity or to a Group of which the User is a member]**.

FDP_ACF.1b.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **[the User is a member of the Administrators Group]**.

FDP_ACF.1b.4 The TSF shall explicitly deny access of subjects to objects based on the **[no additional rules]**.

5.1.3 Identification and authentication (FIA)

5.1.3.1 User attribute definition (FIA_ATD.1a)

FIA_ATD.1a.1 The TSF shall maintain the following list of security attributes belonging to ~~individual~~ **local** users: **[Identity, Groups, Records Management Roles, Function Access Rights, Security Classification, Security Descriptors, Password]**.

5.1.3.2 User attribute definition (FIA_ATD.1b)

FIA_ATD.1b.1 The TSF shall maintain the following list of security attributes belonging to ~~individual~~ **host** users: **[Identity, Groups, Records Management Roles, Function Access Rights, Security Classification, Security Descriptors]**.

***Application Note**: For both local users (FIA_ATD.1a) and host users (FIA_ATD.1b), the attribute "Records Management Roles" is defined and applicable only if the TOE is configured to enforce the Role-Based Access Control SFP.*

5.1.3.3 User attribute definition (FIA_ATD.1c)

FIA_ATD.1c.1 The TSF shall maintain the following list of security attributes belonging to individual ~~users~~ **host applications**: **[Identity, Password]**.

5.1.3.4 User authentication before any action (FIA_UAU.2a)

FIA_UAU.2a.1 The TSF shall require each **local** user **and host application** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user **or application**.

5.1.3.5 User identification before any action (FIA_UID.2)

FIA_UID.2.1 The TSF shall require each user **and host application** to identify itself before allowing any other TSF-mediated actions on behalf of that user **or application**.

5.1.4 Security management (FMT)

5.1.4.1 Management of security functions behavior (FMT_MOF.1)

FMT_MOF.1.1 The TSF shall restrict the ability to **[*determine the behavior of*, *modify the behavior of*]** the functions **[access control]** to **[Administrator, Users with the System Configuration Management Function Access Right]**.

5.1.4.2 Management of security attributes (FMT_MSA.1a – ACL-Based Access Control)

FMT_MSA.1a.1 The TSF shall enforce the **[ACL-Based Access Control SFP]** to restrict the ability to **[*change_default*]** the security attributes **[Access Control List]** to **[Administrator, Users with the File Plan Administration and Security Management Function Access Rights]**.

5.1.4.3 Management of security attributes (FMT_MSA.1b – ACL-Based Access Control)

FMT_MSA.1b.1 The TSF shall enforce the **[ACL-Based Access Control SFP]** to restrict the ability to **[*modify*]** the security attributes **[Access Control List]** to **[Administrator, Custodian, Users with 'Change Permissions' permission if 'Restrict security changes for components to custodians' not set, Users with the Life Cycle Management Design Function Access Right]**.

5.1.4.4 Management of security attributes (FMT_MSA.1c – ACL-Based Access Control)

FMT_MSA.1c.1 The TSF shall enforce the **[ACL-Based Access Control SFP]** to restrict the ability to **[*modify*]** the security attributes **[File Plan Component Security Classification, File Plan Component Security Descriptors]** to **[Administrator, Custodian, Users in Access Control List if 'Restrict security changes for components to custodians' not set]**.

5.1.4.5 Management of security attributes (FMT_MSA.1d – ACL-Based Access Control)

FMT_MSA.1d.1 The TSF shall enforce the **[ACL-Based Access Control SFP]** to restrict the ability to **[*change_default, modify*]** the security attributes **[Field Level Permissions]** to **[Administrator, Users with the Field Level Security Management Function Access Right]**.

5.1.4.6 Management of security attributes (FMT_MSA.1e – Role-Based Access Control)

FMT_MSA.1e.1 The TSF shall enforce the **[Role-Based Access Control SFP]** to restrict the ability to **[*change_default*]** the security attributes **[Access Control List]** to **[Administrator, Users with the File Plan Administration and Security Management Function Access Rights]**.

5.1.4.7 Management of security attributes (FMT_MSA.1f – Role-Based Access Control)

FMT_MSA.1f.1 The TSF shall enforce the **[Role-Based Access Control SFP]** to restrict the ability to **[*modify*]** the security attributes **[Access Control List]** to **[Administrator, Custodian, Users with 'Change Permissions' permission if 'Restrict security changes for components to custodians' not set]**.

5.1.4.8 Management of security attributes (FMT_MSA.1g – Role-Based Access Control)

FMT_MSA.1g.1 The TSF shall enforce the **[Role-Based Access Control SFP]** to restrict the ability to **[*change_default, modify*]** the security attributes **[Role Permissions]** to **[Administrator, Users with the Security Management Function Access Right]**.

5.1.4.9 Management of security attributes (FMT_MSA.1h – Role-Based Access Control)

FMT_MSA.1h.1 The TSF shall enforce the **[Role-Based Access Control SFP]** to restrict the ability to **[*modify*]** the security attributes **[File Plan Component Security Classification, File Plan Component Security Descriptors]** to **[Administrator, Custodian, Users in Access Control List (other than 'Public' Group) if 'Restrict security changes for components to custodians' not set]**.

5.1.4.10 Management of security attributes (FMT_MSA.1i – Role-Based Access Control)

FMT_MSA.1i.1 The TSF shall enforce the **[Role-Based Access Control SFP]** to restrict the ability to **[*change_default, modify*]** the security attributes **[Field Level Permissions]** to **[Administrator, Users with the Field Level Security Management Function Access Right]**.

5.1.4.11 Management of security attributes (FMT_MSA.1j – ACL- and Role-Based Access Control)

FMT_MSA.1j.1 The TSF shall enforce the **[ACL-Based Access Control SFP, Role-Based Access Control SFP]** to restrict the ability to **[*modify, delete, /*assign*/*]** the security attributes **[Custodian]** to **[Administrator, Users with the File Plan Administration Function Access Right (and that also have 'View' and 'Update' permissions for the File Plan Component)]**.

5.1.4.12 Static attribute initialization (FMT_MSA.3a – ACL-Based Access Control)

FMT_MSA.3a.1 The TSF shall enforce the **[ACL-Based Access Control SFP]** to provide **[/inherited/]** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3a.2 The TSF shall allow the **[no role]** to specify alternative initial values to override the default values when an object or information is created.

5.1.4.13 Static attribute initialization (FMT_MSA.3b – Role-Based Access Control)

FMT_MSA.3b.1 The TSF shall enforce the **[Role-Based Access Control SFP]** to provide **[/inherited/]** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3b.2 The TSF shall allow the **[no role]** to specify alternative initial values to override the default values when an object or information is created.

5.1.4.14 Management of TSF data (FMT_MTD.1a – User Accounts and Groups)

FMT_MTD.1a.1 The TSF shall restrict the ability to **[*modify, delete*, /create, activate, deactivate/]** the **[User Accounts (excluding modifying the Password attribute), Groups]** to **[Administrator, Users with the Users/Groups Management Function Access Right]**.

5.1.4.15 Management of TSF data (FMT_MTD.1b – Roles)

FMT_MTD.1b.1 The TSF shall restrict the ability to **[*modify, delete, /*create*/*]** the **[Records Management Roles]** to **[Administrator, Users with the Users/Groups Management Function Access Right]**.

5.1.4.16 Management of TSF data (FMT_MTD.1c – User Passwords)

FMT_MTD.1c.1 The TSF shall restrict the ability to **[*modify*]** the **[Password of another user]** to **[Administrator, Users with the Users/Groups Management Function Access Right]**.

5.1.4.17 Management of TSF data (FMT_MTD.1d – Security Classification Hierarchy)

FMT_MTD.1d.1 The TSF shall restrict the ability to **[*modify*]** the **[Security Classification hierarchy]** to **[Administrator, Users with the Security Classification Management Function Access Right]**.

5.1.4.18 Management of TSF data (FMT_MTD.1e – Security Descriptors)

FMT_MTD.1e.1 The TSF shall restrict the ability to **[*modify, delete, [*create*/]*]** the **[Security Descriptors]** to **[Administrator, Users with the Security Descriptors Management Function Access Right]**.

5.1.4.19 Management of TSF data (FMT_MTD.1f – Minimum Password Length)

FMT_MTD.1f.1 The TSF shall restrict the ability to **[*modify*]** the **[minimum Password length]** to **[Administrator, Users with the User/Groups Management and System Configuration Management Function Access Rights]**.

5.1.4.20 Management of TSF data (FMT_MTD.1g – Auditable Events)

FMT_MTD.1g.1 The TSF shall restrict the ability to **[*query, modify*]** the **[set of auditable events]** to **[Administrator, Users with the Audit Management Function Access Right]**.

5.1.4.21 Time-limited authorization (FMT_SAE.1)

FMT_SAE.1.1 The TSF shall restrict the capability to specify an expiration time for **[Password]** to **[Administrator, Users with the User/Groups Management and System Configuration Management Function Access Right].**

FMT_SAE.1.2 For each of these security attributes, the TSF shall be able to **[prevent the user from logging on except for forcing the user to modify their Password]** after the expiration time for the indicated security attribute has passed.

5.1.4.22 Specification of Management Functions (FMT_SMF.1)

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: **[**

a) **Determine and modify behavior of access control function**
b) **Change default values of and modify File Plan Component security attributes**
c) **Assign, modify, and delete File Plan Component Custodian**
d) **Create, modify, delete, activate and deactivate User Accounts and Groups**
e) **Create, modify and delete Records Management Roles**
f) **Modify the Security Classification hierarchy**
g) **Create, modify and delete Security Descriptors**
h) **Modify minimum Password length and specify Password expiration time**
i) **Query and modify set of auditable events]**.

5.1.4.23 Security roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles **[Administrator, Custodian, Users with 'Change Permissions' permission to a File Plan Component, Users with any of the following Function Access Rights:**

- **File Plan Administration;**
- **Field Level Security Management;**
- **Life Cycle Management Design;**
- **Security Management;**
- **Users/Groups Management;**
- **Audit Management;**
- **Audit Reporting;**

- **System Configuration Management;**
- **Security Classification Management;**
- **Security Descriptors Management]**.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

5.1.5 Protection of the TSF (FPT)

5.1.5.1 Non-bypassability of the TSP (FPT_RVM.1)

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.2 IT Environment Security Functional Requirements

The following table describes the SFRs satisfied by the IT environment of IBM Records Manager V8.4.

Requirement Class	Requirement Component
FAU: Security audit	FAU_STG.1b : Protected audit trail storage
FCS: Cryptographic support	FCS_COP.1 : Cryptographic operation
FDP: User data protection	FDP_ITT.1 : Basic internal transfer protection
FIA: Identification and authentication	FIA_UAU.2b : User authentication before any action
FPT: Protection of the TSF	FPT_ITC.1: Inter-TSF confidentiality during transmission
	FPT_ITT.1: Basic internal TSF data transfer protection
	FPT_SEP.1: IT Environment Domain Separation
	FPT_STM.1: Reliable time stamps

Table 2 IT Environment Security Functional Components

5.2.1 Security audit (FAU)

5.2.1.1 Protected audit trail storage (FAU_STG.1b)

FAU_STG.1b.1 The ~~TSF~~ **IT Environment** shall protect the stored audit records from unauthorised deletion.

FAU_STG.1b.2 The ~~TSF~~ **IT Environment** shall be able to **[*prevent*]** unauthorised modifications to the stored audit records in the audit trail.

5.2.2 Cryptographic support (FCS)

5.2.2.1 Cryptographic operation (FCS_COP.1)

FCS_COP.1.1 The ~~TSF~~ **IT Environment** shall perform [**password encryption and decryption**] in accordance with a specified cryptographic algorithm [**AES-CBC**] and cryptographic key sizes [**128 bits**] that meet the following: [**FIPS 197 (AES)**].

5.2.3 User data protection (FDP)

5.2.3.1 Basic internal transfer protection (FDP_ITT.1)

FDP_ITT.1.1 The ~~TSF~~ **IT Environment** shall enforce the **[ACL-Based Access Control SFP, Role-Based Access Control SFP]** to prevent the **[*disclosure, modification*]** of user data when it is transmitted between physically-separated parts of the TOE.

5.2.4 Identification and authentication (FIA)

5.2.4.1 User authentication before any action (FIA_UAU.2b)

FIA_UAU.2b.1 The ~~TSF~~ **IT Environment** shall require each **host** user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.2.5 Protection of the TSF (FPT)

5.2.5.1 FPT_ITC.1 Inter-TSF confidentiality during transmission

FPT_ITC.1.1 The ~~TSF~~ **IT Environment** shall protect all TSF data transmitted **between** ~~from~~ the TSF ~~to~~ and a remote trusted IT product from unauthorised disclosure **and modification** during transmission.

5.2.5.2 FPT_ITT.1 Basic internal TSF data transfer protection

FPT_ITT.1.1 The ~~TSF~~ **IT Environment** shall protect TSF data from [***disclosure***, ***modification***] when it is transmitted between separate parts of the TOE.

5.2.5.3 IT Environment Domain Separation (FPT_SEP.1)

FPT_SEP.1.1 The ~~TSF~~ **IT Environment** shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The ~~TSF~~ **IT Environment** shall enforce the separation between the security domains of subjects in the TSC.

5.2.5.4 Reliable time stamps (FPT_STM.1)

FPT_STM.1.1 The ~~TSF~~ **IT Environment** shall be able to provide reliable time stamps for **the TOE's and** its own use.

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the EAL 3 augmented with ALC_FLR.2 components as specified in Part 3 of the Common Criteria. No operations are applied to the assurance components.

Requirement Class	Requirement Component
ACM: Configuration management	ACM_CAP.3: Authorization controls
	ACM_SCP.1: TOE CM coverage
ADO: Delivery and operation	ADO_DEL.1: Delivery procedures
	ADO_IGS.1: Installation, generation, and start-up procedures
ADV: Development	ADV_FSP.1: Informal functional specification
	ADV_HLD.2: Security enforcing high-level design
	ADV_RCR.1: Informal correspondence demonstration
AGD: Guidance documents	AGD_ADM.1: Administrator guidance
	AGD_USR.1: User guidance
ALC: Life cycle support	ALC_DVS.1: Identification of security measures
	ALC_FLR.2: Flaw reporting procedures
ATE: Tests	ATE_COV.2: Analysis of coverage
	ATE_DPT.1: Testing: high-level design
	ATE_FUN.1: Functional testing
	ATE_IND.2: Independent testing – sample

Requirement Class	Requirement Component
AVA: Vulnerability assessment	AVA_MSU.1: Examination of guidance
	AVA_SOF.1: Strength of TOE security function evaluation
	AVA_VLA.1: Developer vulnerability analysis

Table 3 EAL 3 Assurance Components

5.3.1 Configuration management (ACM)

5.3.1.1 Authorisation controls (ACM_CAP.3)

ACM_CAP.3.1d The developer shall provide a reference for the TOE.
ACM_CAP.3.2d The developer shall use a CM system.
ACM_CAP.3.3d The developer shall provide CM documentation.
ACM_CAP.3.1c The reference for the TOE shall be unique to each version of the TOE.
ACM_CAP.3.2c The TOE shall be labelled with its reference.
ACM_CAP.3.3c The CM documentation shall include a configuration list and a CM plan.
ACM_CAP.3.4c The configuration list shall uniquely identify all configuration items that comprise the TOE.
ACM_CAP.3.5c The configuration list shall describe the configuration items that comprise the TOE.
ACM_CAP.3.6c The CM documentation shall describe the method used to uniquely identify the configuration items that comprise the TOE.
ACM_CAP.3.7c The CM system shall uniquely identify all configuration items that comprise the TOE.
ACM_CAP.3.8c The CM plan shall describe how the CM system is used.
ACM_CAP.3.9c The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.
ACM_CAP.3.10c The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.
ACM_CAP.3.11c The CM system shall provide measures such that only authorised changes are made to the configuration items.
ACM_CAP.3.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.1.2 TOE CM coverage (ACM_SCP.1)

ACM_SCP.1.1d The developer shall provide a list of configuration items for the TOE.
ACM_SCP.1.1c The list of configuration items shall include the following: implementation representation and the evaluation evidence required by the assurance components in the ST.
ACM_SCP.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2 Delivery and operation (ADO)

5.3.2.1 Delivery procedures (ADO_DEL.1)

ADO_DEL.1.1d The developer shall document procedures for delivery of the TOE or parts of it to the user.
ADO_DEL.1.2d The developer shall use the delivery procedures.
ADO_DEL.1.1c The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.
ADO_DEL.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2.2 Installation, generation, and start-up procedures (ADO_IGS.1)

ADO_IGS.1.1d The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.
ADO_IGS.1.1c The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation and start-up of the TOE.

ADO_IGS.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1.2e The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.3.3 Development (ADV)

5.3.3.1 Informal functional specification (ADV_FSP.1)

ADV_FSP.1.1d The developer shall provide a functional specification.

ADV_FSP.1.1c The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.1.2c The functional specification shall be internally consistent.

ADV_FSP.1.3c The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.

ADV_FSP.1.4c The functional specification shall completely represent the TSF.

ADV_FSP.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2e The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

5.3.3.2 Security enforcing high-level design (ADV_HLD.2)

ADV_HLD.2.1d The developer shall provide the high-level design of the TSF.

ADV_HLD.2.1c The presentation of the high-level design shall be informal.

ADV_HLD.2.2c The high-level design shall be internally consistent.

ADV_HLD.2.3c The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.2.4c The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.2.5c The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.2.6c The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.2.7c The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

ADV_HLD.2.8c The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_HLD.2.9c The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.

ADV_HLD.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_HLD.2.2e The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.3.3.3 Informal correspondence demonstration (ADV_RCR.1)

ADV_RCR.1.1d The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

ADV_RCR.1.1c For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

ADV_RCR.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4 Guidance documents (AGD)

5.3.4.1 Administrator guidance (AGD_ADM.1)

AGD_ADM.1.1d The developer shall provide administrator guidance addressed to system administrative personnel.

AGD_ADM.1.1c The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2c The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3c The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4c The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.

AGD_ADM.1.5c The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6c The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7c The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8c The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

AGD_ADM.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4.2 User guidance (AGD_USR.1)

AGD_USR.1.1d The developer shall provide user guidance.

AGD_USR.1.1c The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2c The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3c The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4c The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.

AGD_USR.1.5c The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6c The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

AGD_USR.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5 Life cycle support (ALC)

5.3.5.1 Identification of security measures (ALC_DVS.1)

ALC_DVS.1.1d The developer shall produce development security documentation.

ALC_DVS.1.1c The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

ALC_DVS.1.2c The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

ALC_DVS.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DVS.1.2e The evaluator shall confirm that the security measures are being applied.

5.3.5.2 Flaw reporting procedures (ALC_FLR.2)

ALC_FLR.2.1d The developer shall provide flaw remediation procedures addressed to TOE developers.
ALC_FLR.2.2d The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.
ALC_FLR.2.3d The developer shall provide flaw remediation guidance addressed to TOE users.
ALC_FLR.2.1c The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.
ALC_FLR.2.2c The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.
ALC_FLR.2.3c The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.
ALC_FLR.2.4c The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.
ALC_FLR.2.5c The flaw remediation procedures shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE
ALC_FLR.2.6c The procedures for processing reported security flaws shall ensure that any reported flaws are corrected and the correction issued to TOE users.
ALC_FLR.2.7c The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.
ALC_FLR.2.8c The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.
ALC_FLR.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.6 Tests (ATE)

5.3.6.1 Analysis of coverage (ATE_COV.2)

ATE_COV.2.1d The developer shall provide an analysis of the test coverage.
ATE_COV.2.1c The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.
ATE_COV.2.2c The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.
ATE_COV.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.6.2 Testing: high-level design (ATE_DPT.1)

ATE_DPT.1.1d The developer shall provide the analysis of the depth of testing.
ATE_DPT.1.1c The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.
ATE_DPT.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.6.3 Functional testing (ATE_FUN.1)

ATE_FUN.1.1d The developer shall test the TSF and document the results.
ATE_FUN.1.2d The developer shall provide test documentation.
ATE_FUN.1.1c The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.
ATE_FUN.1.2c The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.
ATE_FUN.1.3c The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4c The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5c The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

ATE_FUN.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.6.4 Independent testing – sample (ATE_IND.2)

ATE_IND.2.1d The developer shall provide the TOE for testing.

ATE_IND.2.1c The TOE shall be suitable for testing.

ATE_IND.2.2c The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

ATE_IND.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2e The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3e The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.3.7 Vulnerability assessment (AVA)

5.3.7.1 Examination of guidance (AVA_MSU.1)

AVA_MSU.1.1d The developer shall provide guidance documentation.

AVA_MSU.1.1c The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AVA_MSU.1.2c The guidance documentation shall be complete, clear, consistent and reasonable.

AVA_MSU.1.3c The guidance documentation shall list all assumptions about the intended environment.

AVA_MSU.1.4c The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

AVA_MSU.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_MSU.1.2e The evaluator shall repeat all configuration and installation procedures to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.

AVA_MSU.1.3e The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

5.3.7.2 Strength of TOE security function evaluation (AVA_SOF.1)

AVA_SOF.1.1d The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

AVA_SOF.1.1c For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2c For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

AVA_SOF.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_SOF.1.2e The evaluator shall confirm that the strength claims are correct.

5.3.7.3 Developer vulnerability analysis (AVA_VLA.1)

AVA_VLA.1.1d The developer shall perform a vulnerability analysis.

AVA_VLA.1.2d The developer shall provide vulnerability analysis documentation.

AVA_VLA.1.1c The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP.

AVA_VLA.1.2c The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.

AVA_VLA.1.3c The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

AVA_VLA.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VLA.1.2e The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

6. TOE Summary Specification

This chapter describes the security functions and associated assurance measures.

6.1 TOE Security Functions

6.1.1 Security audit

The TOE generates audit records for the following auditable events:

- Start-up and shutdown of the audit functions
- Authentication attempts
- Successful administrative actions including management and configuration of the access control policy.

Each audit record will include the date and time of the event, type of event and user ID of the event. The TOE only records successful events with the exception of the authentication attempts. The TOE records all authentication attempts. The Audit Configuration feature records activities for users and file plan components. For example, it records when a user logs on, adds, updates or deletes a component. It can also record administrative actions such as user and group management activities (i.e., add or update a user account), and file plan component permission changes.

The Records Manager records the configured information and saves it in the audit table. Administrators and users with the Audit Management function access right can select which auditable events are to be audited, based on event type. The auditable event types (or 'items') are: User; Group; Custom Component; Life Cycle; System Component; and Partition. The following table identifies the auditable actions associated with each audit event type:

Event Type	Actions
User	Add, Update, Delete, Logon, Logoff, Failed Logon, Life Cycle Management Event, and Report
Group	Add, Update, Delete, View, and Change Membership
Custom Component	Add, Update, Delete, View, Life Cycle Transition, Move, Host Retrieve, Print, Reserve, Security Classification Info History, Charge Out, Change Suspend, and Change Permissions
Life Cycle	Add, Update, Delete, View
System Component	Add, Update, Delete, View, Logon, Logoff, Failed Logon, Life Cycle Management Event, and Report
Partition	Add, Update, Delete, View, Life Cycle Transition, and Print

Administrators can generate audit entry reports using the advanced query feature to sort the audit data based on user identity and event type. The audit entry reports are presented in a readable and understandable format. Only Administrators and users with both the Audit Reporting and Audit Management function access rights can run audit entry reports. Only Administrators and users with the Audit Management function access right can delete audit entries through the TOE's interfaces. The TOE does not provide any capability through its own interfaces to modify audit entries. However, the TOE also relies on the IT environment to protect audit records from unauthorized modification or deletion and to provide reliable time stamps for recording the date and time in audit records.

The Security audit function is designed to satisfy the following security functional requirements:

- FAU_GEN.1: Audit Records are generated for the appropriate security relevant events and include the date and time of the event, type of event, user identity and outcome of the event.

- FAU_GEN.2: The audit record associates each auditable event with the identity of the user that caused the event.
- FAU_SAR.1: The TOE provides authorized administrators with the ability to read and interpret audit data.
- FAU_SAR.2: The TOE allows only authorized administrators to read the audit records.
- FAU_SAR.3: The TOE provides the ability to perform searches and sorting of audit data based on user ID and event type.
- FAU_SEL.1: The TOE provides the capability to select which auditable events are to be audited, based on event type.
- FMT_MTD.1g: The TOE restricts the capability to query and modify the set of auditable events to Administrators and users with the Audit Management function access right.
- FAU_STG.1a: The interfaces provided by the TOE restrict the capability to purge audit records to Administrators and users with the Audit Management function access right. The TOE does not provide any interfaces for modifying audit records.

6.1.2 User data protection

6.1.2.1 Introduction

The TOE controls user access to file plan components by enforcing an access control policy. The access control policy can be configured in one of two permission modes: Access Control List (ACL); or Role-based. These modes are incompatible, and once one mode has been selected during TOE installation or upgrade, it is not possible to convert to the other permission mode. However, the overall process for determining if access is allowed is the same, regardless of the configured mode.

A user that is a member of the Administrators group has full access to all file plan components. For all other users, the process the TOE implements to determine if access is granted is as follows:

- The TOE first checks if the user has the File Plan Administration function access right, either directly or through group or records management role membership. This function access right grants the user the capability (but not permission) to perform operations on file plan components. If the user does not have this function access right, the user is unable to perform any operation on file plan components
- The TOE then determines what permissions, if any, the user has to access the file plan component. For the ACL-based access control policy, this is based on the user's identity and group memberships and the permissions assigned to users and groups in the file plan component's ACL. For the role-based access control policy, this is based on the user's records management role memberships and the permissions assigned to records management roles in the file plan component definition. The TOE determines if the user is allowed to perform the requested operation based on the user's permissions. However, if the user is a custodian of the file plan component, the user automatically has all permissions to the file plan component and the TOE bypasses this check
- Under Role-based access control, the TOE separately determines if the user is allowed to access the file plan component, based on the user's identity and group memberships and the set of users and groups specified in the file plan component's ACL. However, if the user is a custodian of the file plan component, the user automatically has access to the file plan component and the TOE bypasses this check
- Next, the TOE determines if the user has the appropriate security classification and security descriptors to access the file plan component

If these checks all pass, the TOE allows the requested operation to be performed on the file plan component. However, the TOE also checks if any field level permissions are set on individual fields of the file plan component, determines if they are applicable to the requested operation (only Add and Update are applicable), and if so determines if the user has permission to perform the requested operation on the protected fields.

The following sections provide further details about the various aspects of the access control policy.

6.1.2.2 Permissions

The TOE defines the following permissions that can be granted to users to control the operations the user can perform on file plan components:

Permission	Description
Add	To add a file plan component of a particular type
Update (Edit)	To update or modify an existing file plan component of a particular type
Delete	To remove a file plan component of a particular type from the file plan itself
View	To see the profile of a file plan component of a particular type. Users who cannot view a file plan component will not know of its existence in the file plan
Suspend	To suspend a file plan component from transitioning through its life cycle
UnSuspend	To remove a suspension from a file-plan component and allow it to continue through its life cycle
Move	To move a file plan component from one place in the file plan to another
Change Permissions	To alter the permissions assigned to a particular file plan component
Reserve	To reserve a file plan component for yourself, or for someone else
Add Link	To add a link
Delete Link	To delete a link
Charge Out	To charge out a file plan component to yourself, or to someone else
Host Retrieve	To retrieve a record to a user's workspace on their computer when the file plan component represents a record stored in an adjoining host application. This permission is stored in IBM Records Manager for information purposes only, since IBM Records Manager cannot directly control whether an adjoining application allows a user to retrieve a document
Add Partition	To segment container type components
Delete Partition	To remove a partition

6.1.2.3 Custodians

A custodian (either a user or a group) can be assigned to a file plan component to restrict the management of access controls on that file plan component (the custodian is system attribute of each file plan component). A user that is a custodian of a file plan component automatically has all permissions to that file plan component (but is still subject to all other access checks). The TOE restricts the ability to assign, modify, and delete the custodian of a file plan component to the Administrator and to users with the File Plan Administration function access right and 'View' and 'Update' permissions for that file plan component.

By default, the TOE does not check custodianship when processing a request to change permissions on a file plan component. If the TOE is configured to restrict security changes for components to custodians, then when a user (or group) has custodianship of a file plan component, no other user (with the exception of an Administrator) can modify the access controls applied to that component. The custodian is inheritable. A user or group that is assigned custodianship of a file plan component also has custodianship of all the descendants of that component.

6.1.2.4 ACL Permission Mode

The ACL-Based Access Control Policy uses an Access Control List (ACL) to determine the users and groups that can access a file plan component and with what permissions. An ACL entry comprises a user or group and the permissions granted to that user or group for the file plan component. The TOE compares the user's identity and group memberships with entries in the ACL. A user's permissions are the combination of the permissions assigned

in the ACL directly to the user and the permissions assigned in the ACL to all the groups of which the user is a member.

There are four ways in which permissions can be set:

- **System wide**—also known as just "system permissions", these are applied to file plan component definitions and provide what in effect are default permissions for all file plan components
- **Component level**—permissions set on a specific file plan component, which override any system permissions
- **Phase level**—permissions assigned to a life cycle phase, which override any system and component level permissions
- **Field level**—the **Add** and **Update** permissions can be set for individual fields within a file plan component.

When a component is added to a file plan, it inherits all permissions from its container. The container's permissions were derived either from the system or from its container, which in turn derived its permissions from the system or its container, and so on, until the top of the file plan is reached.

When permissions are set for a file plan component (i.e., Component level), these permissions are then inherited by all the descendants of that file plan component, with the exception of file plan components that have different permissions explicitly defined for them. The file plan component where the permissions are set is called the **permissions owner**. The descendant file plan components below the permissions owner are called the **permissions inheritors**. A file plan component where no permissions are set explicitly is automatically a permissions inheritor. When permissions are specified for a file plan component, that file plan component automatically becomes a permissions owner. Any permissions inheritor file plan components below the new permissions owner automatically inherit their permissions from the new permissions owner.

The TOE provides two options that change this behavior when permissions are set on a file plan component:

- **Reset Descendants**—replaces the permissions of all the descendants of a component, including those components with their own explicitly defined permissions, with the current component's permissions (essentially, all descendant components become permissions inheritors)
- **Inherit from Parent**—sets the permissions of the component to the permissions of its parent. The component's descendants inherit their parent's permissions, unless they have their own explicitly defined permissions. This provides a simple way to reset a component's permissions to those of its parent (essentially, the component changes from a permissions owner to a permissions inheritor).

When the initial (root) file plan component is created, there are no permissions assigned to it, so only the Administrator has access to the component. Furthermore, until either system permissions are set, or permissions are set on the root file plan component, all new file plan components that inherit their parent's permissions will also not be accessible to anyone but the Administrator.

If a file plan component is assigned a life cycle and enters a life cycle phase on which permissions are defined, those permissions override both system and component permissions and stay with the file plan component. If the component is set to move into successive phases, it will assume the permission rules of each phase (if set) and will discard the permissions of any previous phase. If there are no permissions set in a phase, when the component moves into that phase, its permissions remain untouched (for example, it retains whatever permissions were last assigned to it). A user requires the Life Cycle Management Design function access right in order to be able to define and modify phase level permissions.

Field level permissions can optionally be specified on individual fields within a file plan component. The two field level permissions that can be specified are **Add** and **Update**. The Add permission, when specified on a field, gives the list of specified users and groups the right to provide the value for that field when adding a new file plan component. The Update permission, when specified on a field, gives the list of specified users and groups the right to provide a new value for that field when updating the file plan component. The administrator specifies field level permissions in a file plan component definition and they apply when a user adds or updates a file plan component of that type.

6.1.2.5 Role-based Permissions Mode

If the TOE has been configured to enforce the Role-Based Access Control Policy, then permissions are assigned to records management roles that apply throughout the file plan hierarchy. Before a user can perform an operation on a file plan component, the user must have both "permission" and "access", which are granted independently:

- **Permission to perform the operation**—the user requires specific file plan permissions (such as **View** and **Update**) for that operation, which are granted in the file plan component definition, and are based on the user's records management role
- **Access to the component**—the user must be granted explicit access to that file plan component, either directly, or as a member of a group. Access is granted by identifying the user or group in the file plan component's ACL, which is inherited by its descendants.

The Administrator defines the records management roles (also identified by the TOE and guidance documentation as "primary groups") and can assign to each records management role any desired function access rights and Security Descriptors. The Administrator can then assign records management roles, and the permissions granted to each role, to file plan component definitions. A records management role can have different permissions for different file plan component definitions. A user assigned to a records management role will have the permissions to a file plan component that are granted to the role at the file plan component definition. However, in order to access a specific file plan component, the user must also be granted access to that file plan component, either directly or as a member of a group. In order to change permissions, a user must have the "Change Permissions" permission assigned to their role. Furthermore, if the TOE is configured to restrict security changes for components to their custodians, the user must also be the custodian, or there must not be a custodian assigned, in order for the user to be able to change permissions on a file plan component.

Under the Role-Based Access Control Policy, field level permissions can be granted to users and groups, similarly to the way field level permissions can be granted to users and groups under the ACL-Based Access Control Policy. The user's records management role is not involved in determining if field level permissions are granted, only the user's identity and group memberships.

6.1.2.6 Security Classifications

The TOE supports hierarchical security classifications that are assigned to file plan components and users. When the TOE is installed, it defines a single security classification (Unclassified). Administrators are able to define hierarchical security classifications to represent the business requirements of the TOE owner. Security classifications are defined by a name and a number, assigned by the Administrator—the higher the number, the higher in the hierarchy is the classification. Comparing classifications for the purpose of determining access is therefore a numeric comparison based on the numbers assigned to the classifications.

By default, every user is allocated the lowest level security classification in the hierarchy, which defines their clearance level (this will be 'Unclassified' if the Administrator has not defined a classification hierarchy). File plan components are also assigned a security classification, the default being the lowest level in the hierarchy (again, this will be 'Unclassified' if the Administrator has not defined a classification hierarchy). Users cannot access file plan components classified at a higher level than their current security clearance level.

The security classification assigned to a file plan component is not governed by the "Change Permissions" permission. If a user has access to the file plan component (either directly or as a member of a group), the user is allowed to change the security classification, provided:

- The file plan component does not have a custodian, or
- The file plan component has a custodian but the TOE is not configured to restrict security changes for components to custodians.

6.1.2.7 Security Classification Consistency Level

The TOE provides the capability to set the **Security Classification Consistency Level** attribute to configure a view of the file plan to behave according to a specified consistency level. This capability allows the Administrator to choose a file plan component definition (for which the current view is the primary view) where the security

classification will be maintained. This attribute only applies for hierarchical views, and always favors the higher security classification. It should be noted that the classification changes apply to the file plan components, not just the view of the components.

The **Security Classification Consistency Level** has the following classification options:

a) Automatically upgrade component's children to component level

b) Automatically upgrade component to highest level of children

c) Both.

If security consistency is configured, the following rules apply:

- If a child component is added with a lower level of security than its parent, the child's security level is upgraded to that of its parent [a) and c)]
- If a child component is added with a higher level of security than its parent, the parent's security will be upgraded to that of the child [b) and c)]; if "Both" classification options have been selected, this will then cause the security level of all the existing child components to be upgraded to the parent's level
- After the creation of a file plan component at the level where security classification consistency is configured, its security classification level cannot be changed to a level that is lower than the level of its child components [a), b) and c)]. However, there is a system configuration setting to Allow downgrade with security consistency, which when set overrides this rule. In this case, if a container component is downgraded, all its children will have their security downgraded to the same level as the container component.

6.1.2.8 Security Descriptors

Security descriptors are markings that elaborate on or clarify document handling, for example "Contracts" or "Personnel". The TOE allows Administrators to define security descriptors that can then be assigned to file plan components, users, groups, and records management roles (if the Role-Based Permissions model is in use). A file plan component can have multiple security descriptors allocated to it. All descendant components inherit their parent's security descriptors. The way in which the TOE handles access decisions based on security descriptors depends on the **Security descriptor control access level**, which can have one of the following values:

- **Strict**—Users are not able to access the file plan component if they do not have all the descriptors required for that file plan component (this is the default setting)
- **Always warn**—Users are able to access the file plan component but receive a warning message if they do not have all the descriptors allocated to that file plan component
- **Warn when File Plan Component is Owner**—Users are able to access the file plan component but receive a warning when the file plan component is the owner of the descriptor (the owner is the file plan component to which the descriptors were originally assigned, i.e., the file plan component did not inherit the descriptors)
- **Off**—Descriptors are ignored and become purely informational.

The security descriptors assigned to a file plan component are not governed by the "Change Permissions" permission. If a user has access to the file plan component (either directly or as a member of a group), the user is allowed to change the security descriptors, provided:

- The file plan component does not have a custodian, or
- The file plan component has a custodian but the TOE is not configured to restrict security changes for components to custodians.

Security classifications and security descriptors provide an additional means for restricting access, supplemental to the ACL or Role-Based Permissions models. Users still need to be granted the necessary permissions to a file plan component in order to perform a requested operation, even if they have the correct security classification and/or correct set of security descriptors. In other words, even if a user has the correct security classification and/or security

descriptors, if the file plan component doesn't grant the user access, the user will be unable to access the file plan component.

The User data protection function is designed to satisfy the following security functional requirements:

- FDP_ACC.2a, FDP_ACF.1a: When configured for ACL-Based access control, the TOE enforces the ACL-Based Access Control SFP on all users and file plan components and the operations users can perform on file plan components. Access is authorized based on the permissions granted to the user by the file plan component ACL, the user and file plan component security classifications, and the user and file plan component security descriptors.
- FDP_ACC.2b, FDP_ACF.1b: When configured for Role-Based access control, the TOE enforces the Role-Based Access Control SFP on all users and file plan components and the operations users can perform on file plan components. Access is authorized based on the permissions granted to the user's assigned records management roles, the user being granted access by the file plan component ACL, the user and file plan component security classifications, and the user and file plan component security descriptors.
- FMT_MSA.3a, FMT_MSA.3b: Under both the ACL-Based and Role-Based Access Control SFPs, file plan components inherit their security attributes from their parent component when they are created. There is no capability to specify alternative initial values of security attributes when the file plan component is created.
- FMT_MSA.1a, FMT_MSA.1e: Both the ACL-Based and Role-Based Access Control SFPs support default permissions that are applied at the level of file plan component definitions. These system permissions can be changed only by an Administrator or a user with both the File Plan Administration and Security Management function access right.
- FMT_MSA.1b: The ACL-Based Access Control SFP restricts the ability to modify a file plan component ACL to an Administrator, the file plan component Custodian, a user with Change Permissions permission on the file plan component (provided 'Restrict security changes for components to custodians' has not been set), or a user with the Life Cycle Management Design function access right. Users with the Life Cycle Management Design function access right are able to define phase level permissions on life cycle phases. The assignment of phase level permissions occurs automatically when a file plan component enters a life cycle phase on which phase level permissions are defined, and those permissions will override both system and component level permissions.
- FMT_MSA.1c: The ACL-Based Access Control SFP restricts the ability to modify a file plan component's security classification and security descriptors to an Administrator, the file plan component Custodian, or a user granted access to the file plan component by being identified in the file plan component's ACL (provided 'Restrict security changes for components to custodians' has not been set).
- FMT_MSA.1h: The Role-Based Access Control SFP restricts the ability to modify a file plan component's security classification and security descriptors to an Administrator, the file plan component Custodian, or a user granted access to the file plan component by being identified in the file plan component's ACL (other than the Public group, and provided 'Restrict security changes for components to custodians' has not been set).
- FMT_MSA.1d, FMT_MSA.1i: Both the ACL-Based and Role-Based Access Control SFPs support field level permissions that are specified at the level of the file plan component definition. By default, field level access is not restricted, and field level permissions can be set and changed only by an Administrator or a user with the Field Level Security Management function access right.
- FMT_MSA.1f: The Role-Based Access Control SFP restricts the ability to modify a file plan component ACL to an Administrator, the file plan component Custodian, or a user with Change Permissions permission on the file plan component (provided 'Restrict security changes for components to custodians' has not been set).
- FMT_MSA.1g: The Role-Based Access Control SFP supports default records management role-based permissions that are applied at the level of file plan component definitions. These permissions can be changed only by an Administrator or a user with the Security Management function access right.

- FMT_MSA.1j: Both the ACL-Based and Role-Based Access Control SFPs restrict the ability to assign, modify, and delete a file plan component Custodian to an Administrator or a user with the File Plan Administration function access right and 'View' and 'Update' permission on the file plan component.
- FMT_MOF.1: The TOE provides the following configuration options that affect the behavior of the access control function: 'Restrict security changes for components to custodians'; 'Security descriptor control access level'. The ability to determine the setting of and modify these options is restricted to an Administrator or a user with the System Configuration Management function access right.

6.1.3 Identification and authentication

All users of the TOE must have a user account defined in the TOE. The TOE maintains a set of security attributes for each user that includes user identity, group membership, records management roles, password, function access rights, security classification, and security descriptors.

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. When a local user logs on, they must provide their unique identification and password before any further access to the TOE is granted.

A host user is created and exists within the host application. Host users can access the TOE in two ways, as follows:

- from within the host application—in this case, the TOE needs only to know the identity of the host user. It assumes that the host application has already authenticated the user. The host application logs itself into the TOE via the API, then supplies the user identification on calls to the API for TOE services
- by logging on to the TOE—in this case, the host user selects the host they belong to and uses 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 system allows for the configuration of the maximum duration for a password and the minimum length of a password. By default, the minimum password length is set at 8 characters. Administrator guidance advises not setting this below 8 characters. Guidance documentation also advises that passwords should have a maximum length of 25 characters. User passwords have a time-stamp associated with them, and after the specified number of days, the user is not able to log on. When a user attempts to log on with an expired password, they will receive an error indicating that they must change their password. The TOE will provide the interface for the user to change their password before access to the TOE is granted. The TOE will verify that the user entered the expired password and the new password. The TOE will also verify that the new password is at least the minimum specified length. User accounts can be configured so that their password never expires. In addition, an Administrator can flag an account to ensure that the user changes their password the next time he or she logs on (even when his or her password has not yet expired).

The TOE uses AES, implemented in the WebSphere Application server (WAS) Java Development Kit (JDK) in the IT environment (in compliance with FIPS140-2), to encrypt a user's password before storing it in the TOE database.

The Identification and authentication function is designed to satisfy the following security functional requirements:

- FIA_ATD.1a: The TOE maintains the following list of security attributes for local users: user identity, group membership, records management roles, password, function access rights, security classification, and security descriptors.
- FIA_ATD.1b: The TOE maintains the following list of security attributes for host users: user identity, group membership, records management roles, function access rights, security classification, and security descriptors.
- FIA_ATD.1c: The TOE maintains the following list of security attributes for host applications: host application identity, password.

- FIA_UAU.2a: The TOE requires each user to be successfully authenticated before they are granted access to the TOE and any of its functions.
- FIA_UID.2: The TOE requires each user to be successfully identified before they are granted access to the TOE and any of its functions.
- FMT_MTD.1f: The TOE provides the capability to set a minimum length for user passwords. This capability is restricted to an Administrator or a user with both the Users/Groups Management and System Configuration Management function access rights.
- FMT_SAE.1: The TOE provides the capability to set an expiration time for user passwords. Once a user's password expires, the user must change their password before being allowed to log on to the TOE. The capability to set the maximum password age is restricted to an Administrator or a user with both the Users/Groups Management and System Configuration Management function access rights.

6.1.4 Security management

The TOE uses **function access rights** to control access to its features, including security management functions. If a user does not have the appropriate function access right for a feature, the user has no access to the feature and cannot perform any actions associated with the feature. For example, a user requires the File Plan Administration function access right in order to perform actions on file plan components, regardless of what permissions, security classification and security descriptors they have been granted.

The TOE defines the following function access rights—note that those marked with an asterisk ('*') confer some security management capability on the user granted that function access right:

***Audit Management**—To configure individual events that are not audited.

Disposal Authorities—To create, edit, or delete disposal authorities.

File Plan Design—To design file plans.

Browse File Plan—To browse file plans.

***File Plan Administration**—To add elements to a file plan, including the ability to add, edit, or delete individual file plan components.

***Life Cycle Management Design**—To define life cycle codes, life cycle phases, and other life cycle management items, including assigning phase level permissions.

Life Cycle Management Operation—To execute life cycle management operations, such as disposition.

Pick List Management—To create, edit, or delete pick lists.

Profile Design—To create, edit, and delete data entry profiles (forms) for all objects, including file plan components, and system objects.

***Security Management**—To define permissions at a global level.

***Security Descriptors Management**—To create, update and delete Security descriptors.

***Security Classification Management**—To create, update and delete Security classification

Security Classification Reasons Management—To create, update and delete Security classification reasons.

Security Classification Exemptions Management—To create, update and delete Security classification exemption.

Security Classification Guide Management—To create, update and delete Security classification guide.

***Users/Groups Management**—To add, edit or delete users and groups along with the ability to add users to groups.

Records Host Management—To add, edit or delete the record-host identifiers that define a record host to the Records Manager. A record host is an application with which the Records Manager is integrated and that acts as the repository of the records managed by the Records Manager.

Extensions Management—To create, edit, and delete extensions that extend the functionality of the base Records Manager.

Reservation Management—To create, update and delete reservations.

Charge-Out Management—To create, update and delete charge outs.

Auto-Classify Rules Management—To define auto-classification rules.

Default Management—To create, edit, and delete defaults for different file plan component definitions.

***System Configuration Management**—To customize the behavior of IBM Records Manager.

Report Layout Management—To assign and delete report layouts.

Report Search Management—To open, delete, and assign saved public searches to users and groups.

***Field Level Security Management**—To determine the users that can change field level permissions.

***Audit reporting** – To determine the users that can report on audit.

Purge Audit Entries – To purge the audit entries.

View ALL audit entries – To determine the users that can view the audit entries.

During installation, the TOE creates a built-in user account, "Administrator", and a built-in group, "Administrators", which has "Administrator" as its only member. The Administrators group is given all function access rights, which are then inherited by the Administrator user. The authorized administrators of the TOE are users that are assigned to the Administrators group (including Administrator) and users and groups that are granted function access rights that provide access to security management functions.

The full name, the login name, and the password of the default Administrator user can be altered by an Administrator. However, the Administrator user's access rights cannot be modified and the account itself cannot be deleted. Furthermore, while the name of the Administrators group can be modified, its function access rights cannot be modified, the Administrator user cannot be removed from it, and it cannot be deleted.

The TOE also defines a generic group account called the Public group. The Public group contains all of the users defined in the TOE. Any new users added to the TOE automatically become members of the Public group. Administrators can assign function access rights, security descriptors and component permissions (via component ACLs) to the Public group, but cannot directly add members to, or delete members from this group.

The IRM Web Admin provides the interface with the options the authorized administrators will use to perform the security management functions. The options that handle the security management functions include the following:

- The Tools option provides authorized administrators the ability to: query and modify the set of auditable events; determine and modify the behavior of the access control function; and provides the interface for users to change their passwords
- The Search option provides authorized administrators the ability to review the audit records in a report format
- The Security option provides authorized administrators with capabilities to:
    - create, modify, delete, activate and deactivate a user account or group (a user will be unable to login if their account is deactivated; deactivation takes affect after a user logs out)
    - create, modify and delete a records management role
    - modify the security classification hierarchy
    - create, modify, and delete security descriptors
    - set how long a user's password is valid and the minimum password length
- The File Plan Administration and Security options provide authorized administrators the capability to change default values of and modify file plan component security attributes

- The File Plan Administration option provides authorized administrators the capability to assign, modify and delete file plan component custodians.

The Security management function is designed to satisfy the following security functional requirements:

- FMT_MTD.1a: The TOE provides the capability to create, modify, delete, activate and deactivate user accounts and groups, and restricts this capability (with the exception of modifying user passwords—every user can modify their own password) to an Administrator or a user with the Users/Group Management function access right.
- FMT_MTD.1b: The TOE provides the capability to create, modify and delete records management roles and restricts this capability to an Administrator or a user with the Users/Group Management function access right.
- FMT_MTD.1c: The TOE restricts this capability to modify another user's password to an Administrator or a user with the Users/Group Management function access right.
- FMT_MTD.1d: The TOE provides the capability to modify the security classification hierarchy. This capability is restricted to an Administrator or a user with the Security Classification Management function access right.
- FMT_MTD.1e: The TOE provides the capability to create, modify and delete security descriptors. This capability is restricted to an Administrator or a user with the Security Descriptor Management function access right.
- FMT_SMF.1: The TOE provides the following security management functions:
    - Determine and modify behavior of access control function
    - Change default values of and modify File Plan Component security attributes
    - Assign, modify and delete the File Plan Component Custodian
    - Create, modify, delete, activate and deactivate User Accounts and Groups
    - Create, modify and delete Records Management Roles
    - Modify the Security Classification hierarchy
    - Create, modify and delete Security Descriptors
    - Modify minimum Password length and specify Password expiration time
    - Query and modify set of auditable events.
- FMT_SMR.1: The TOE defines the security management role of Administrator by creating the Administrators group during installation and allocating it all function access rights. A user granted any of the following function access rights also has some security management capability:
    - Field Level Security Management
    - Security Management
    - Users/Groups Management
    - Audit Management
    - Audit Reporting
    - System Configuration Management
    - Security Classification Management
    - Security Descriptors Management.

  A user must be granted the File Plan Administration function access right in order to interact with the file plan components. This function access right can, in combination with the Security Management function access right or the 'Change Permissions' permission, also grant some security management capability. The

TOE also supports the security management role of custodian for file plan components, which can be used to restrict management of permissions on file plan components.

6.1.5 Protection of the TSF

The TOE ensures that the TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed. The TSF requires that all local users be successfully identified and authenticated before any operations can be performed on the system. The TSF requires all host users to be identified, but assumes that the host application has authenticated their users. The TSF also requires each host application to be identified and authenticated. Once these steps are completed successfully, the authorized user has access only to functions as specified by his or her assigned function access rights. Every attempt to operate on a file plan component is mediated by the access control policy configured for the TOE (either the ACL-Based Access Control Policy or the Role-Based Access Control Policy).

In addition to ensuring that the TSF is appropriately protected, the IT environment is expected to provide reliable timestamps for use by the TSF and a secure domain to execute the TOE. The IT environment is also relied on to protect TSF and user data transmitted between TOE components and between the TOE and non-TOE components. In an AIX-based environment, this is achieved using a VPN, while a Windows-based environment uses IPSEC. The IT environment supports SSL to protect communication between a web browser and the IRM Web Admin component.

The Protection of the TSF function is designed to satisfy the following security functional requirements:

- FPT_RVM.1: The TOE ensures that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

6.2 TOE Security Assurance Measures

6.2.1 Configuration management

The configuration management measures applied by IBM ensure that configuration items are uniquely identified, and that documented procedures are used to control and track changes that are made to the TOE. IBM ensures changes to the implementation representation are controlled. IBM performs configuration management on the TOE implementation representation, design documentation, tests and test documentation, user and administrator guidance, delivery and operation documentation, life-cycle documentation, vulnerability analysis documentation, and configuration management documentation. All of these items are identified in the configuration management plan as configuration items.

These activities are documented in:

- IBM Records Manager v8.4 Configuration Management.

The Configuration management assurance measure satisfies the following EAL 3 assurance requirements:

- ACM_CAP.3
- ACM_SCP.1.

6.2.2 Delivery and operation

IBM provides delivery documentation and procedures to identify the TOE, secure the TOE during delivery, and provide necessary installation and generation instructions. IBM's delivery procedures describe all applicable procedures to be used to prevent in appropriate access to the TOE. IBM also provides documentation that describes the steps necessary to install IBM Records Manager V8.4 in accordance with the evaluated configuration.

These activities are documented in:

- IBM Records Manager V8.4 Delivery Operation and Guidance

- IBM Records Manager Planning and Installing Your Record Management System Version 8 Release 4.

The Delivery and operation assurance measure satisfies the following EAL 3 assurance requirements:

- ADO_DEL.1
- ADO_IGS.1.

6.2.3 Development

IBM has numerous documents describing all facets of the design of the TOE. In particular, they have a functional specification that describes the accessible TOE interfaces; a high-level design that decomposes the TOE architecture into subsystems and describes each subsystem and their interfaces; and, correspondence documentation that explains how each of the design abstractions correspond from the TOE summary specification in the Security Target to the subsystems.

These activities are documented in:

- IBM Records Manager Version 8.4 Security High-level Functional Specification and Design
- RM 84_DesignDocMapping.

The Development assurance measure satisfies the following EAL 3 assurance requirements:

- ADV_FSP.1
- ADV_HLD.2
- ADV_RCR.1.

6.2.4 Guidance documents

IBM provides administrator and user guidance on how to utilize the TOE security functions and warnings to administrators and users about actions that can compromise the security of the TOE. The procedures included in the administrator guidance describe the steps necessary to operate the TOE in accordance with the evaluated configuration, detailing how to establish and maintain the secure configuration.

The user guidance describes the procedures to use the TOE security-related functions that are available to the non-administrative users. The procedures describe how to utilize the functions and the associated interfaces in the evaluated configuration.

The guidance documentation includes guidance on how to integrate host applications with the TOE in order to correctly use the records management capability of the TOE.

These activities are documented in:

- IBM Records Manager System Administration Guide Version 8 Release 4
- Addendum to the IBM Records Manager System Administration Guide.

The Guidance documents assurance measure satisfies the following EAL 3 assurance requirements:

- AGD_ADM.1
- AGD_USR.1.

6.2.5 Life cycle support

IBM applies security controls on the development environment that are adequate to provide the confidentiality and integrity of the TOE design and implementation that is necessary to ensure the secure development of the TOE.

The documentation describes the physical, procedural, personnel, and other development security measures that are used in the development environment to protect the TOE. It includes the physical security of the development

location and any procedures used to select development staff. It further describes the procedures utilized to track all reported security flaws, the status on correcting the flaw and what measures are being taken to correct the flaw.

These activities are documented in:

- IBM Records Manager V8.4 Lifecycle document.

The Life cycle support assurance measure satisfies the following EAL 3 assurance requirements:

- ALC_DVS.1
- ALC_FLR.2.

6.2.6 Tests

IBM has a test plan that describes how each of the necessary security functions is tested, along with the expected test results. IBM has documented each test as well as an analysis of test coverage and depth demonstrating that the security aspects of the design evident from the functional specification and high-level design are appropriately tested. Actual test results are created on a regular basis to demonstrate that the tests have been applied and that the TOE operates as designed.

These activities are documented in:

- IBM Records Manager v8.4 Security Related Test Plan
- IBM Records Manager v8.4 Security Related Test Cases.

The Tests assurance measure satisfies the following EAL 3 assurance requirements:

- ATE_COV.2
- ATE_DPT.1
- ATE_FUN.1
- ATE_IND.2.

6.2.7 Vulnerability assessment

The TOE administrator and user guidance documents describe the operation of IBM Records Manager V8.4 and how to maintain a secure state. These guides also describe all necessary operating assumptions and security requirements outside the scope of control of the TOE. They have been developed to serve as complete, clear, consistent, and reasonable administrator and user references.

IBM has conducted a strength of function analysis wherein all permutational or probabilistic security mechanisms have been identified and analyzed resulting in a demonstration that all of the relevant mechanisms fulfill the minimum strength of function claim, SOF-Basic.

IBM performs regular vulnerability analyses of the entire TOE (including documentation) to identify obvious weaknesses that can be exploited in the TOE.

These activities are documented in:

- IBM Records Manager Version 8.4 Vulnerability Analysis.

The Vulnerability assessment assurance measure satisfies the following EAL 3 assurance requirements:

- AVA_MSU.1
- AVA_SOF.1
- AVA_VLA.1.

7. Protection Profile Claims

There are no Protection Profile claims in this Security Target.

8. Rationale

This section provides the rationale for completeness and consistency of the Security Target. The rationale addresses the following areas:

- Security Objectives
- Security Functional Requirements
- Security Assurance Requirements
- Strength of Functions
- Requirement Dependencies
- TOE Summary Specification
- PP Claims.

8.1 Security Objectives Rationale

This section shows that all secure usage assumptions and threats are completely covered by security objectives. In addition, each objective counters or addresses at least one assumption or threat.

8.1.1 Security Objectives Rationale for the TOE and Environment

This section provides evidence demonstrating the coverage of threats and usage assumptions by the security objectives.

	T.AUDIT	T.NOAUTH	T.OBJ_ACCESS	A.AUTH_DATA	A.NOEVIL	A.SECURE_ENV	A.PROTECT
O.AUDIT	X						
O.AUTHORIZE		X	X				
O.AUTH_DATA		X					
O.MANAGE		X					
O.OBJ_ACCESS			X				
O.SELPRO		X	X				
OE.SEP		X					
OE.TIME	X						
OE.TRANSFER			X				
OE.HOST_AUTH		X	X				
OE.ADMIN					X		
OE.AUTH_DATA				X			
OE.INSTALL						X	
OE.PHYS							X

Table 4 Environment to Objective Correspondence

8.1.1.1 T.AUDIT

Authorized users of the TOE may not be held accountable for their actions within the TOE.

This threat is countered by ensuring that:

- O.AUDIT: The TOE provides the means to record and review an audit trail of security related events such that authorized users are held accountable for their security relevant actions.
- OE.TIME: The IT environment supports the TOE audit capability by providing reliable time stamps.

8.1.1.2 T.NOAUTH

An unauthorized user may gain access to the TOE and its resources in order to bypass, deactivate, or tamper with TOE security functions.

This threat is countered by ensuring that:

- O.AUTH_DATA: The TOE will provide the ability for authorized non-administrative users to modify their own authentication data.
- O.AUTHORIZE: The TOE will ensure that only authorized users and administrators gain access to the TOE and its resources.
- O.MANAGE: The TOE will only allow administrators to access and manage the TOE security functions.
- O.SELPRO: The TOE will protect itself against attempts by unauthorized users to bypass or deactivate TOE security functions.
- OE.SEP: The TOE operating environment shall provide mechanisms to isolate the TSF and assure that TSF components cannot be tampered with or bypassed.
- OE.HOST_AUTH: The host application shall authenticate each user it defines before allowing any other host-mediated actions on behalf of that user, thus ensuring that only authorized users can gain access to TOE services and resources via the host application.

8.1.1.3 T.OBJ_ACCESS

An unauthorized user may gain access to objects maintained by the TOE in order to modify or destroy them.

This threat is countered by ensuring that:

- O.AUTHORIZE: The TOE will ensure that only authorized users and administrators gain access to the TOE and its resources.
- O.OBJ_ACCESS: The TOE will limit access to objects maintained by the TOE to users with authorization and appropriate privileges. The TOE will allow authorized users to specify which users may access their objects and the actions performed on the objects.
- O.SELPRO: The TOE will protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.
- OE.HOST_AUTH: The host application shall authenticate each user it defines before allowing any other host-mediated actions on behalf of that user, thus ensuring that only authorized users can gain access to TOE services and resources via the host application.
- OE.TRANSFER: The IT environment will ensure that the data transmitted between the TOE components is protected from tampering and disclosure.

8.1.1.4 A.AUTH_DATA

Authorized users of the TOE will keep all their authentication data private.

This assumption is satisfied by ensuring that:

- OE.AUTH_DATA: Those responsible for the TOE will ensure that all access credentials such as passwords or other authentication information, are protected by the users in a manner consistent with IT security objectives.

8.1.1.5 A.NOEVIL

The administrative personnel are competent, not careless, willfully negligent, or hostile and will follow and abide by the instructions provided by TOE documentation.

This assumption is satisfied by ensuring that:

- OE.ADMIN: Authorized administrators are competent, not careless, willfully negligent, or hostile and will follow and abide by the instructions provided by TOE documentation..

8.1.1.6 A.SECURE_ENV

The IT infrastructure 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.

This assumption is satisfied by ensuring that:

- OE.INSTALL: Those responsible for the TOE will ensure that the TOE and its operating environment is delivered, installed, managed and operated in a manner that is consistent with TOE security objectives.

8.1.1.7 A.PROTECT

TOE will be located within controlled facilities which will prevent unauthorized physical access and modification.

This assumption is satisfied by ensuring that:

- OE.PHYS: Those responsible for the TOE will ensure that those parts of the TOE critical to security policy are protected from any physical attack.

8.2 Security Requirements Rationale

This section provides evidence supporting the internal consistency and completeness of the components (requirements) in the Security Target. Note that **Table 5** indicates the requirements that effectively satisfy the individual objectives. .

8.2.1 Security Functional Requirements Rationale

All Security Functional Requirements (SFR) identified in this Security Target are fully addressed in this section and each SFR is mapped to the objective for which it is intended to satisfy.

	O.AUDIT	O.AUTHORIZE	O.AUTH_DATA	O.MANAGE	O.OBJ_ACCESS	O.SELPRO	OE.SEP	OE.TIME	OE.TRANSFER	OE.HOST_AUTH
FAU_GEN.1	X									
FAU_GEN.2	X									
FAU_SAR.1	X									
FAU_SAR.2	X									
FAU_SAR.3	X									
FAU_SEL.1	X									
FAU_STG.1a	X									
FAU_STG.1b							X			
FCS_COP.1									X	
FDP_ACC.2a		X			X					
FDP_ACC.2b		X			X					

	O.AUDIT	O.AUTHORIZE	O.AUTH_DATA	O.MANAGE	O.OBJ_ACCESS	O.SELPRO	OE.SEP	OE.TIME	OE.TRANSFER	OE.HOST_AUTH
FDP_ACF.1a		X			X					
FDP_ACF.1b		X			X					
FDP_ITT.1									X	
FIA_ATD.1a		X			X					
FIA_ATD.1b		X			X					
FIA_ATD.1c		X			X					
FIA_UAU.2a		X								
FIA_UAU.2b										X
FIA_UID.2		X								
FMT_MOF.1				X						
FMT_MSA.1a				X	X					
FMT_MSA.1b				X	X					
FMT_MSA.1c				X	X					
FMT_MSA.1d				X	X					
FMT_MSA.1e				X	X					
FMT_MSA.1f				X	X					
FMT_MSA.1g				X	X					
FMT_MSA.1h				X	X					
FMT_MSA.1i				X	X					
FMT_MSA.1j				X	X					
FMT_MSA.3a					X					
FMT_MSA.3b					X					
FMT_MTD.1a			X	X						
FMT_MTD.1b				X						
FMT_MTD.1c			X							
FMT_MTD.1d				X						
FMT_MTD.1e				X						
FMT_MTD.1f				X						
FMT_MTD.1g	X									
FMT_SAE.1				X						
FMT_SMF.1				X						
FMT_SMR.1				X						
FPT_ITC.1									X	
FPT_ITT.1									X	
FPT_RVM.1					X	X				
FPT_SEP.1							X			
FPT_STM.1								X		

Table 5 Objective to Requirement Correspondence

8.2.1.1 O.AUDIT

The TSF must provide the means to record and review an audit trail of security related events such that users can be held accountable for their security relevant actions.

This TOE Security Objective is satisfied by ensuring that:

- FAU_GEN.1: The TOE generates an audit record of all security relevant user actions which includes the date and time of the event.

- FAU_GEN.2: The TOE associates each auditable event with the identity of the user that caused the event which thereby holds the user accountable for their actions.
- FAU_SAR.1: The TOE provides authorized administrative users with the ability to read all audit information.
- FAU_SAR.2: The TOE ensures only authorized administrative users are able to read the audit information.
- FAU_SAR.3: The TOE provides the ability for users to perform searches and sorting of audit data based on user id and event type.
- FAU_SEL.1, FMT_MTD.1g: The TOE provides a means specify what auditable events should be audited, in order to keep the amount of audit data to a manageable amount. The capability to modify the set of auditable events is restricted to authorized administrative users.
- FAU_STG.1a: The TOE ensures the interfaces it provides to the audit data do not allow unauthorized modification or deletion of the audit data through those interfaces.

8.2.1.2 O.AUTHORIZE

The TOE must ensure that only authorized users and administrators gain access to the TOE and its resources.

This TOE Security Objective is satisfied by ensuring that:

- FDP_ACC.2a, FDP_ACC.2b: Depending on its configuration, the TOE enforces either an ACL-Based or a Role-Based Access Control SFP on all subjects and objects and the operations among them.
- FDP_ACF.1a, FDP_ACF.1b: The TOE enforces the ACL-Based or Role-Based Access Control SFP, as appropriate, using rules based on the security attributes of the subjects and objects.
- FIA_ATD.1a: The TOE will maintain a list of security attributes belonging to local users.
- FIA_ATD.1b: The TOE will maintain a list of security attributes belonging to host users.
- FIA_ATD.1c: The TOE will maintain the identity and password for all host applications registered with the TOE.
- FIA_UAU.2a: The TOE requires each local user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. In addition, the TOE requires each host application to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that application.
- FIA_UID.2: The TOE requires each user (both local and host) to be successfully identified before allowing any other TSF-mediated actions on behalf of that user. In addition, the TOE requires each host application to be successfully identified before allowing any other TSF-mediated actions on behalf of that application.

8.2.1.3 O.AUTH_DATA

The TOE must allow authorized users to modify their own authentication data.

This TOE Security Objective is satisfied by ensuring that:

- FMT_MTD.1a, FMT_MTD.1c: Users are always able to modify their own password. The ability to modify any user's password is restricted to authorized administrators.

8.2.1.4 O.MANAGE

The TOE must allow administrators to effectively manage the TOE, and its security functions, and must ensure that only authorized administrators are able to access its functionality.

This TOE Security Objective is satisfied by ensuring that:

- FMT_MOF.1: Only an authorized administrator is allowed to determine and modify the behavior of the access control function.
- FMT_MSA.1a-j: The ability to manage security attributes within the scope of the supported SFP is restricted to an authorized administrator.
- FMT_MTD.1a: The ability to create, modify, delete, activate and deactivate user accounts (with the exception of modifying the Password attribute) and groups is restricted to an authorized administrator.
- FMT_MTD.1b: The ability to create, modify and delete records management roles is restricted to an authorized administrator.

- FMT_MTD.1d: The ability to modify the security classification hierarchy is restricted to an authorized administrator.
- FMT_MTD.1e: The ability to create, modify and delete security descriptors is restricted to an authorized administrator.
- FMT_MTD.1f: The ability to modify the minimum password length is restricted to an authorized administrator.
- FMT_SAE.1: Only the authorized administrator can specify when a user's password will expire and force users to change their password before access to the TOE is granted.
- FMT_SMF.1: The authorized administrator is provided with the capabilities necessary to manage the security functionality of the TOE.
- FMT_SMR.1: The TOE maintains security management roles that are authorized to exercise the capabilities provided to effectively manage the TOE and its security functions.

8.2.1.5 O.OBJ_ACCESS

The TOE must limit access to objects maintained by the TOE to users with authorization and appropriate privileges. The TSF must allow authorized users to specify which users may access their objects and the actions performed on the objects.

This TOE Security Objective is satisfied by ensuring that:

- FDP_ACC.2a, FDP_ACC.2b: Depending on its configuration, the TOE enforces either an ACL-Based or a Role-Based Access Control SFP on all subjects and objects and the operations among them.
- FDP_ACF.1a, FDP_ACF.1b: The TOE enforces the ACL-Based or Role-Based Access Control SFP, as appropriate, using rules based on the security attributes of the subjects and objects.
- FIA_ATD.1a: The TOE will maintain a list of security attributes belonging to local users.
- FIA_ATD.1b: The TOE will maintain a list of security attributes belonging to host users.
- FIA_ATD.1c: The TOE will maintain the identity and password for all host applications registered with the TOE.
- FMT_MSA.1a-j: The ability to manage security attributes within the scope of the supported SFP is restricted to an authorized administrator.
- FMT_MSA.3a: When a new object is created under the ACL-Based Access Control SFP, it inherits its security attributes from its parent object, thus ensuring access to the new object is limited to users authorized to access the parent object.
- FMT_MSA.3b: When a new object is created under the Role-Based Access Control SFP, it inherits its security attributes from its parent object, thus ensuring access to the new object is limited to users authorized to access the parent object.
- FPT_RVM.1: The TOE ensures that the Access Control SFP is invoked and succeeds before any access to TOE objects is granted.

8.2.1.6 O.SELPRO

The TOE must protect itself against attempts by unauthorized users to bypass and deactivate TOE security functions.

This TOE Security Objective is satisfied by ensuring that:

- FPT_RVM.1: The TOE ensures that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

8.2.1.7 OE.SEP

The TOE operating environment shall provide mechanisms to isolate the TSF and assure that TSF components cannot be tampered with or bypassed.

This IT Environment Security Objective is satisfied by ensuring that:

- FAU_STG.1b: The IT environment protects the audit data from unauthorized modification or deletion.

- FPT_SEP.1: The IT environment maintains and enforces a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

8.2.1.8 OE.TIME

The IT environment shall provide an accurate timestamp.

This IT Environment Security Objective is satisfied by ensuring that:

- FPT_STM.1: The IT environment provides a reliable time stamp for use of the TOE in its audit records.

8.2.1.9 OE.TRANSFER

The IT environment shall ensure the data transmitted between TOE components and between the TOE and non-TOE components is protected from tampering and disclosure.

This IT Environment Security Objective is satisfied by ensuring that:

- FDP_ITT.1: The IT environment will protect the user data transmitted between the components of the TOE from disclosure and modification.
- FPT_ITC.1: The IT environment will protect the TSF data transmitted between the TOE and non-TOE components.
- FPT_ITT.1: The IT environment will protect the TSF data transmitted between the components of the TOE.
- FCS_COP.1: The IT environment includes a FIPS 140-2 validated cryptographic module that provides cryptographic algorithms to support encryption of TSF data stored and transmitted by the TOE.

8.2.1.10 OE.HOST_AUTH

The host application shall authenticate each user that it defines before allowing any other host-mediated actions on behalf of that user.

This IT Environment Security Objective is satisfied by ensuring that:

- FIA_UAU.2b: The IT environment shall require each host user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

8.3 Security Assurance Requirements Rationale

This ST contains the assurance requirements for CC EAL3 augmented with ALC_FLR.2. The EAL chosen is based on the statement of the security environment (threats, assumptions, and organizational policy) and the security objectives defined in this ST. The augmentation was chosen to provide the added assurance acquired by defining flaw remediation procedures and correcting security flaws. The sufficiency of the EAL chosen (EAL3) is justified based on those aspects of the environment that have impact upon the assurance needed in the TOE. The administrative staff is conscientious, non-hostile and well trained (A.NOEVIL, A.TRAINED_STAFF, and OE.ADMIN, OE.TRAINED_STAFF) and all users of the TOE protect all access control data (i.e. password) (A.AUTH_DATA, OE.AUTH_DATA). The TOE is physically protected (A.PROTECT, OE.PHYS), and properly and securely configured (A.OS, OE.INSTALL). Given these aspects, a TOE based on good commercial development and maintenance practices is sufficient. EAL3 augmented is an appropriate level of assurance for the TOE described in this ST.

8.4 Strength of Functions Rationale

IBM Records Manager V8.4 is targeted at a generalized IT environment with good physical access security and competent administrators, for which EAL3 is an appropriate level of assurance. For such TOEs, a minimum strength of function claim of Basic is consistent with the intended environment and target evaluation level. Note that the only applicable mechanism (i.e., one that is probabilistic or permutational) is related to user and host application authentication (FIA_UAU.2a).

8.5 Requirement Dependency Rationale

The following table identifies each security functional requirement in this ST. The table enumerates the dependencies of each requirement as specified in the CC and then identifies the requirement in this ST that satisfies each of those dependencies. Note that in some cases a dependency is satisfied by a hierarchically (as defined in the CC) greater requirement component (identified in **bold**) or by a requirement specified on the IT environment (identified in *italics*). Note that a requirement that is both a hierarchically greater component and specified on the IT environment is identified in ***bold italics***. Where a dependency is unsatisfied, rationale for not satisfying the dependency is provided following the table.

ST Requirement	CC Dependencies	ST Dependencies
FAU_GEN.1	FPT_STM.1	*FPT_STM.1*
FAU_GEN.2	FAU_GEN.1, FIA_UID.1	FAU_GEN.1, **FIA_UID.2**
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1
FAU_SEL.1	FAU_GEN.1, FMT_MTD.1	FAU_GEN.1, FMT_MTD.1g
FAU_STG.1a	FAU_GEN.1	FAU_GEN.1
FCS_COP.1	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1), FCS_CKM.4, FMT_MSA.2	See rationale
FDP_ACC.2a	FDP_ACF.1	FDP_ACF.1a
FDP_ACC.2b	FDP_ACF.1	FDP_ACF.1b
FDP_ACF.1a	FDP_ACC.1, FMT_MSA.3	**FDP_ACC.2a**, FMT_MSA.3a
FDP_ACF.1b	FDP_ACC.1, FMT_MSA.3	**FDP_ACC.2b**, FMT_MSA.3b
FIA_ATD.1a	none	none
FIA_ATD.1b	none	none
FIA_ATD.1c	none	none
FIA_UAU.2a	FIA_UID.1	**FIA_UID.2**
FIA_UAU.2b	FIA_UID.1	**FIA_UID.2**
FIA_UID.2	none	none
FMT_MOF.1	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_MSA.1a	FMT_SMR.1, FMT_SMF.1, (FDP_ACC.1 or FDP_IFC.1)	FMT_SMR.1, FMT_SMF.1, **FDP_ACC.2a**
FMT_MSA.1b	FMT_SMR.1, FMT_SMF.1, (FDP_ACC.1 or FDP_IFC.1)	FMT_SMR.1, FMT_SMF.1, **FDP_ACC.2a**
FMT_MSA.1c	FMT_SMR.1, FMT_SMF.1, (FDP_ACC.1 or FDP_IFC.1)	FMT_SMR.1, FMT_SMF.1, **FDP_ACC.2a**
FMT_MSA.1d	FMT_SMR.1, FMT_SMF.1, (FDP_ACC.1 or FDP_IFC.1)	FMT_SMR.1, FMT_SMF.1, **FDP_ACC.2a**
FMT_MSA.1e	FMT_SMR.1, FMT_SMF.1, (FDP_ACC.1 or FDP_IFC.1)	FMT_SMR.1, FMT_SMF.1, **FDP_ACC.2b**
FMT_MSA.1f	FMT_SMR.1, FMT_SMF.1, (FDP_ACC.1 or FDP_IFC.1)	FMT_SMR.1, FMT_SMF.1, **FDP_ACC.2b**
FMT_MSA.1g	FMT_SMR.1, FMT_SMF.1, (FDP_ACC.1 or FDP_IFC.1)	FMT_SMR.1, FMT_SMF.1, **FDP_ACC.2b**
FMT_MSA.1h	FMT_SMR.1, FMT_SMF.1, (FDP_ACC.1 or FDP_IFC.1)	FMT_SMR.1, FMT_SMF.1, **FDP_ACC.2b**
FMT_MSA.1i	FMT_SMR.1, FMT_SMF.1, (FDP_ACC.1 or FDP_IFC.1)	FMT_SMR.1, FMT_SMF.1, **FDP_ACC.2b**
FMT_MSA.1j	FMT_SMR.1, FMT_SMF.1, (FDP_ACC.1 or FDP_IFC.1)	FMT_SMR.1, FMT_SMF.1, **FDP_ACC.2a**, **FDP_ACC.2b**
FMT_MSA.3a	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1a, FMT_MSA.1b, FMT_MSA.1c, FMT_MSA.1d, FMT_SMR.1

ST Requirement	CC Dependencies	ST Dependencies
FMT_MSA.3b	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1e, FMT_MSA.1f, FMT_MSA.1g, FMT_MSA.1h, FMT_MSA.1i, FMT_SMR.1
FMT_MTD.1a	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_MTD.1b	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_MTD.1c	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_MTD.1d	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_MTD.1e	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_MTD.1f	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_MTD.1g	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_SAE.1	FMT_SMR.1, FPT_STM.1	FMT_SMR.1, *FPT_STM.1*
FMT_SMF.1	none	none
FMT_SMR.1	FIA_UID.1	**FIA_UID.2**
FPT_RVM.1	none	none
FAU_STG.1b	FAU_GEN.1	FAU_GEN.1
FDP_ITT.1	FDP_ACC.1 or FDP_IFC.1	**FDP_ACC.2a**, **FDP_ACC.2b**
FPT_ITC.1	none	none
FPT_ITT.1	none	none
FPT_SEP.1	none	none
FPT_STM.1	none	none

Functional component FCS_COP.1 has dependencies on (FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1), FCS_CKM.4, and FMT_MSA.2. However, the cryptographic module in the IT environment is FIPS 140-2 validated. Therefore, the dependencies of key generation (or key import), key destruction and secure key values are satisfied by this module's validation as FIPS 140-2 compliant.

8.6 Explicitly Stated Requirements Rationale

There are no explicitly stated requirements in this Security Target.

8.7 TOE Summary Specification Rationale

Each subsection in Section 6, the TOE Summary Specification, describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

This Section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. The security functions described in the TOE summary specification are all necessary for the required security functionality in the TSF. **Table 6 Security Functions vs. Requirements Mapping** demonstrates the relationship between security requirements and security functions.

	Security audit	User data protection	Identification and authentication	Security management	Protection of the TSF
FAU_GEN.1	X				
FAU_GEN.2	X				
FAU_SAR.1	X				
FAU_SAR.2	X				
FAU_SAR.3	X				
FAU_SEL.1	X				
FAU_STG.1a	X				
FDP_ACC.2a		X			
FDP_ACC.2b		X			
FDP_ACF.1a		X			
FDP_ACF.1b		X			
FIA_ATD.1a			X		
FIA_ATD.1b			X		
FIA_ATD.1c			X		
FIA_UAU.2a			X		
FIA_UID.2			X		
FMT_MOF.1		X			
FMT_MSA.1a		X			
FMT_MSA.1b		X			
FMT_MSA.1c		X			
FMT_MSA.1d		X			
FMT_MSA.1e		X			
FMT_MSA.1f		X			
FMT_MSA.1g		X			
FMT_MSA.1h		X			
FMT_MSA.1i		X			
FMT_MSA.1j		X			
FMT_MSA.3a		X			
FMT_MSA.3b		X			
FMT_MTD.1a				X	
FMT_MTD.1b				X	
FMT_MTD.1c				X	
FMT_MTD.1d				X	
FMT_MTD.1e				X	
FMT_MTD.1f			X		
FMT_MTD.1g	X				
FMT_SAE.1			X		
FMT_SMF.1				X	
FMT_SMR.1				X	
FPT_RVM.1					X

Table 6 Security Functions vs. Requirements Mapping

8.8 PP Claims Rationale

See Section 7, Protection Profile Claims.