IBM® DB2® Document Manager V8.4 Fix Pack 1 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

LIST OF TABLES

1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE is IBM® DB2® Document Manager Version 8.4 Fix Pack 1, provided by International Business Machines (IBM). Document Manager provides the capability to manage controlled documents, such as standard operating procedures, engineering drawings, work instructions, and material safety data sheets, throughout the lifecycle of the documents. It enforces a role-based policy that controls what operations users can perform on documents, based on the user's role. Document Manager relies on IBM® DB2® Content Manager Enterprise Edition V8.4 Fix Pack 1a to act as a content repository for Document Manager documents[1].

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 addressed by the TOE and assumptions about the environment and method of use of the TOE.
- Security Objectives (Section 4): This section details the security objectives of the TOE and its environment.
- IT Security Requirements (Section 5): This section presents the security functional requirements (SFRs) for the TOE and the IT environment that supports the TOE, and the security assurance requirements (SARs) against which the TOE is to be evaluated.
- TOE Summary Specification (Section 6): This section describes the security functions the TOE implements to satisfy its SFRs and the assurance measures that satisfy the its SARs.
- Protection Profile Claims (Section 7): This section identifies and justifies any Protection Profile claims made in the ST.
- Rationale (Section 8): This section closes the ST with the justifications of the security objectives, requirements and TOE summary specifications as to their consistency, completeness and suitability.

1.1 Security Target, TOE and CC Identification

ST Title – IBM® DB2® Document Manager V8.4 Fix Pack 1 Security Target

ST Version – ST Version 1.0

ST Date – 8 January 2009

TOE Identification – IBM® DB2® Document Manager Version 8.4 Fix Pack 1

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 Extended

[1] DB2® Document Manager can also work with FileNET Panagon Content Services as a content repository, but this does not support all of the TOE features and so is not included in the evaluated configuration.

- 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

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 …").
- Explicitly stated requirements are identified by the suffix '_EX'
- 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 Users	The users, administrative and non-administrative, who have been given access to the TOE.
Classes	The method of categorizing the document types in the TOE. The class provides the means of defining the business process rules that apply to a document, by associating document states, document management roles, and a document life cycle with the document type.
Content Manager	A database and data management system (content management system) that provides a foundation for managing, accessing, and integrating critical business information on demand.
Document	The basic object managed by the TOE (DB2® Document Manager). Documents are stored as items in the content repository.
Item	The basic object managed in Content Manager. A document is a specific type of item.
State	A single point in a document's life cycle.

1.3.3 Abbreviations

ACL	Access Control List
CAD	Computer Aided Design

CC	Common Criteria
CM	Content Manager
CEM	Common Evaluation Methodology
CCEVS	Common Criteria Evaluation and Validation Scheme
DM	Document Manager
DoD	Department of Defense
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
HLD	High-level Design
IA	Initial Assessment
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OLE	Object Linking and Embedding
PP	Protection Profile
SAIC	Science Applications International Corporation
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control (see TSF below)
TSF	TOE Security Functions
US	United States

2. TOE Description

The Target of Evaluation (TOE) is IBM® DB2® Document Manager Version 8.4 Fix Pack 1, henceforth referred to as Document Manager (or occasionally just 'DM').

2.1 TOE Overview

Document Manager works with IBM® DB2® Content Manager Enterprise Edition V8.4 Fix Pack 1a (also referred to simply as 'Content Manager' or 'CM') to manage controlled documents throughout their lifecycle. Typical controlled documents include standard operating procedures, engineering drawings, work instructions, and material safety data sheets. Document Manager provides relationship management of related documents and manages the various states and transitions that occur throughout a document's lifecycle, from creation to disposition or destruction.

The Document Manager system is built on a three-tiered computing model as follows:

- **Content Repository tier—**provides a foundation for managing, accessing, and integrating critical business information on demand. All Document Manager documents are stored within the underlying Content Manager system. Document Manager does not require additional databases or tables to be created in this case. The Content Manager repository incorporates an underlying database, the IBM DB2 Universal Database™ to manage documents and information[2]. This environment consists of a library server and one or more resource managers. It should be noted that Content Manager works with "items", and that Document Manager documents are one type of item that may be managed in the repository. The library server is responsible for maintaining and controlling information about items in the repository. Access control of the item and item attributes are managed by the library server and the resource manager stores the associated file. This tier is part of the TOE's operating environment, but not part of the TOE.
- **Document Manager Server and Services tier—**the middle tier of the system. This tier comprises several components, some of which are automated services that run at designated intervals. These components interact directly with the Content Repository tier and the Document Manager Desktop tier (see below). The four primary components of the Server and Services tier are:
  - Library Objects (also referred to as DM Server)—control communication with the content repository. All information, including configuration, compound document, rendition, and other Document Manager specific information are stored in the repository.
  - Cache Manager—controls the information (in the form of cache objects) stored in the cache, such as user, document state and class, and menu data. Cache objects are small files that contain configuration information, such as menus, actions, dialogs and folders. The cache files are stored on the Document Manager Server. As changes are made to the Document Manager configurations using the Designer (a tool used to configure the Desktop—see below), Cache Manager updates those configurations in the repository and in the cache files that are stored on the Document Manager Server. The use of cache objects enhances Document Manager Desktop performance by reducing the resource utilization that occurs in client-server applications. Note that Cache Manager runs as a Windows service, is configured from the DM Service Manager, and is thus included in the "Services" bulleted item below. However, it differs from the other DM services in that it provides the generic service of creating and updating the DM cache, which is used by the other DM services. Thus it is described separately here.
  - Services—control specialized task processing. The Document Manager services are specialized applications that run as Windows services. These services comprise: Lifecycle Services; Notification Services; Rendition Services; Print/Plot Services; Automation Services; Alarm Manager; and Cache Manager (see separate bulleted item above).

[2] While Content Manager can incorporate an Oracle database, the evaluated version of Document Manager relies on the evaluated version of IBM® DB2® Content Manager for Enterprise Edition V8.4 Fix Pack 1a, which does not include an Oracle database in the evaluated configuration.

- Client Software Delivery component—controls software installation and updates to the Document Manager Desktop.

- **Document Manager Clients tier**—consists of the following five components:
  - Desktop—a client application that provides a completely configurable environment from which the user can:
    - Organize the workspace
    - Check out and check in, copy, view, and print items in the repository
    - Transition items in the life cycle
    - Integrate with desktop applications to work directly with items in the repository.
  - Application Integration—the DM Desktop exposes DM features from within other applications through application integration. DM supports integration with the Microsoft Office suite (Word, Excel, PowerPoint, Outlook), Lotus Notes, AutoCAD, Microstation, AutoVue and other viewing applications. Note that users cannot interact with the TOE directly from or via end user applications. When an application is "integrated" with the Desktop, it provides a means for the user to access the application from the Desktop and to use the application to work with documents maintained within the TOE. The user still needs to login to the Desktop before being able to access an integrated application from the Desktop.
  - Designer—a system administration client application used to customize the Desktop for users and groups. The authorized administrator is able to create Desktop templates and assign these to users and groups. The Desktop template is used to configure the DB2 Document Manager Desktop for end users. Menus, views, searches, application integration profiles, and native library folder displays are among the many Desktop objects that can be configured and assigned to a user or group via the Desktop template. Desktop templates can be assigned at the system, group, or user level. If a user or group has not been assigned to a Desktop template, the user or group automatically uses the Default Template configuration. Users and groups must be assigned to other templates in order for their DB2 Document Manager Desktop to use the configuration of that template.

    The Designer enables the authorized administrator to configure the Document Manager environment and the Desktop. After the administrator deploys the Desktop to the users, any changes made by the administrator using the Designer are automatically pushed to the Desktop. The Desktop can be configured to implement updates when the next user action is invoked[3] or at the start of the user's next login session.

    Note: The Designer does not require users to identify or authenticate themselves before accessing its capabilities. By default, Designer is installed on the same computer as the DM Server component. This computer is assumed to be located within a controlled access environment that protects it from unauthorized physical access and modification. In addition, during initial configuration of the TOE, the TOE administrator should use Designer to configure a Desktop template that includes the "Configure" command and that is assigned only to a TOE administrator role. Following the initial configuration of the TOE library and the administrator Desktop template, Designer should always be run via the "Configure" command from this administrator Desktop client. This will ensure that the administrator must be identified and authenticated before accessing other TOE capabilities.
  - Item Loader—simplifies the batch loading of items into the repository. The Item Loader not only adds items, but also provides the capability to maintain compound relationships, set access control, load item profile information, add items to specific folders, as well as submit items for life cycle, rendition, or print or plot processing. The Item Loader allows the user to set up default values for specific item and version properties, the access control list, keywords, and folders. Using the Desktop, the user can override these default values for individual selected files.

    The Item Loader has the technology to scan documents for reference files and automatically add the reference files and maintain those relationships within the content repository. It can automatically

[3] This option is not recommended as it has a significant impact on performance, since the cache is checked against the cache server on every attempted operation.

detect relationships between some types of compound documents such as CAD reference files and Object Linking and Embedding (OLE) linked files like spreadsheets linked to word processing documents. The Item Loader supports parent-child links, peer-to-peer links and dynamic links.

- Client API—the COM-based Client API can be used to develop DM plug-ins, application integrations, and completely new applications. It comprises a set of COM objects, interfaces and properties that support early and late binding. It is delivered with the Desktop Client in a self-registering Windows dynamic link library.

2.2 TOE Architecture

The architecture relies on a repository infrastructure as the core component of this model. The Content Repository tier utilizes the IBM DB2® Content Manager repositories. To the end user, these components appear as one seamless extension of their desktop. To the Information Technology (IT) manager, the three-tiered structure provides a scalable system whose parts are distributed so that items are stored close to those who use them most, while still being available to the entire organization. The following diagram depicts the components of Document Manager as described above in the preceding section.

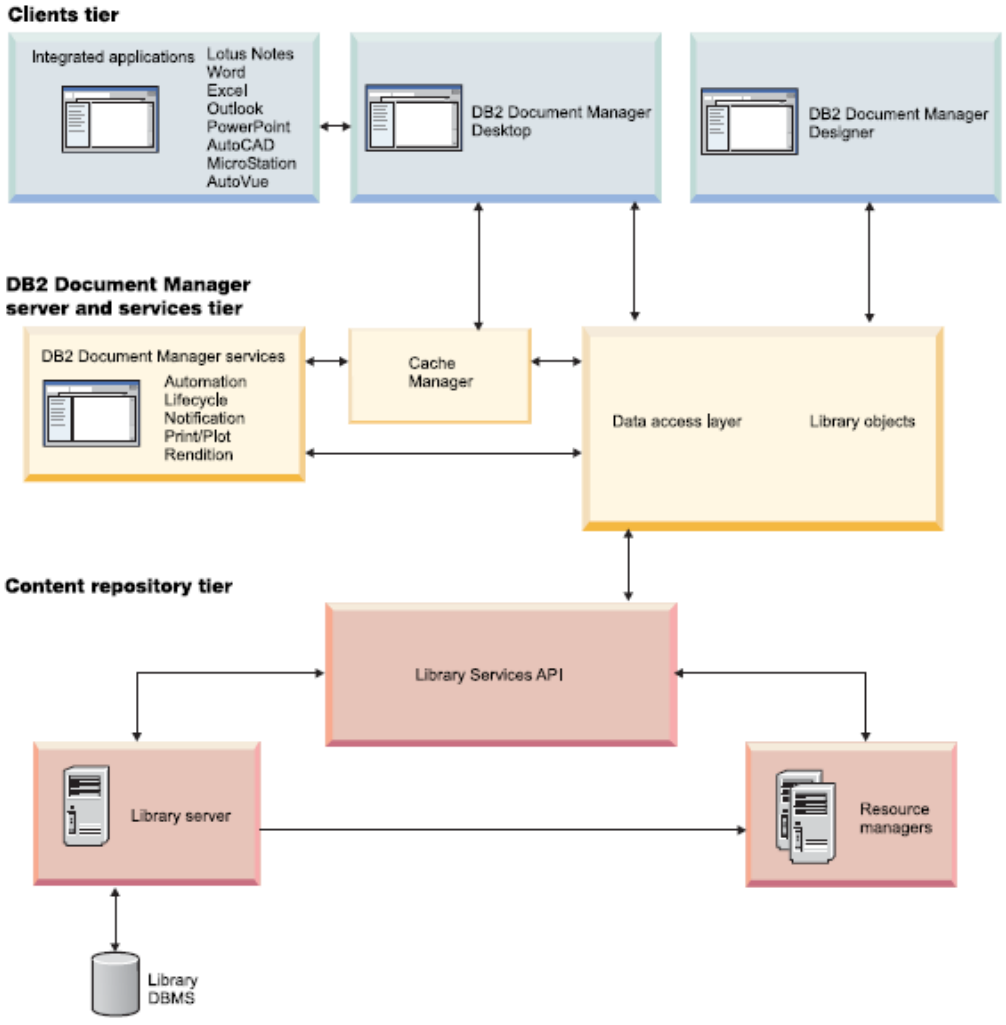

Figure 1. Three-tiered architectural model of the DB2 Document Manager system

In Figure 1, all components within the "DB2 Document Manager server and services tier" and the "DB2 Document Manager Desktop" and "DB2 Document Manager Designer" components in the "Clients tier" are TOE components. Within the "Integrated applications" component in the "Clients tier", the listed applications (Lotus Notes, Word, Excel, etc.) are in the IT environment. All components in the "Content repository tier" are also in the IT environment. Note also that the "Data access layer" encapsulates the "Client Software Delivery" component described in Section 2.1.

2.2.1 Physical Boundaries

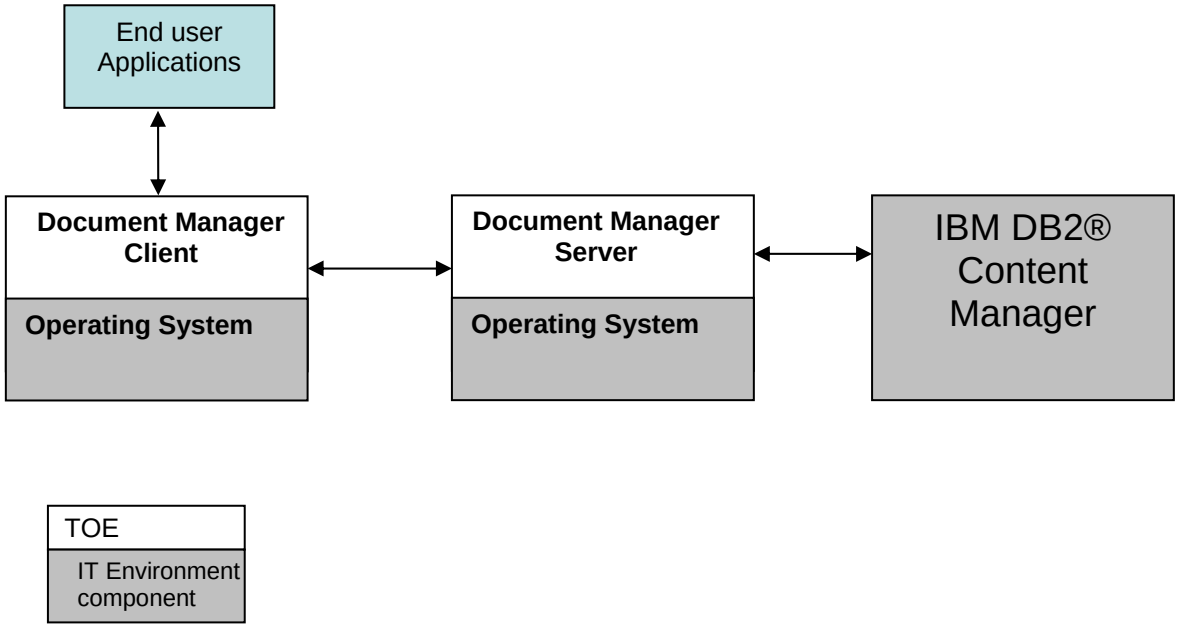

Figure 2: TOE operating environment

Each TOE component operates in the context of its underlying operating system. The TOE relies on its IT environment for the following support:

- To ensure a secure domain for the execution of each TOE component
- To provide a reliable timestamp for audit records
- To protect the stored audit records
- To identify and authenticate users
- To enforce an access control policy on the underlying items stored in the content repository and to provide capabilities to manage that policy
- To define an authorized administrator role that supports security management of both the TOE and the IT environment
- To protect communication between the TOE components and between the TOE and Content Manager.

The following table identifies the IT environment requirements for the DM Server and Services Tier components.

OS	DB2 + fix packs	II4C C++ Connector
Windows Server 2003, Service Pack 2 Windows Server 2003, Service Pack 1 Windows Server 2003, R2 Service Pack 2 Windows Server 2003, R2 Windows 2000 Advanced Server, Service Pack 4 Windows 2000 Server, Service Pack 4	UDB and SDK V9.1 FP3	8.4 Fix pack 1

The following table identifies the IT environment requirements for the DM Clients Tier components:

Software	Level
Windows OS	Windows Vista (Business, Ultimate, and Enterprise Editions (x86 32-bit)) Windows XP Professional, Service Pack 2 Windows XP Professional, Service Pack 1 Windows XP Professional Windows 2000 Professional, Service Pack 4 Windows Server 2003, Service Pack 2 Windows Server 2003, Service Pack 1 Windows Server 2003, R2 Service Pack 2 Windows Server 2003, R2 Windows 2000 Advanced Server, Service Pack 4 Windows 2000 Server, Service Pack 4
Internet Explorer	**On Microsoft Windows Vista and Microsoft Windows XP systems:** Microsoft Internet Explorer 7 **On all supported Microsoft Windows systems:** Microsoft Internet Explorer 6

The following table identifies supported levels of applications that can be integrated with the DM Desktop.

Software	Level
Adobe Acrobat (Distiller)	7.0.9 and 8.1.1
Autodesk AutoCAD	2006, 2007, 2008, 2008 Service Pack 1
Bentley MicroStation J, MicroStation 8, MicroStation 8 XM	J, 8, 8XM
Cimmetry AutoVue client	18, 19.1, 19.1 Service Packs 1 and 2
Lotus Notes	6,5,7,8

Microsoft Office XP, 2003, 2007, 2007 Service Pack 1 • Microsoft Excel • Microsoft Outlook • Microsoft PowerPoint • Microsoft Word	Microsoft Office XP, 2003, 2007, 2007 Service Pack 1
Parametric Technology Corporation (PTC) Arbortext Editor	5.3

The TOE utilizes the Content Manager repository, which is part of the IT environment, to store and manage documents. DM Desktop can be installed on the same computer as DM Server, which means it can be installed on the same computer as DM Designer (Designer is installed with DM Server). DM Desktop can also be installed on a separate computer from the DM Server, which is the most common configuration.

The IT environment should provide the secure channel for communication between the TOE components or between the TOE and Content Manager. In the Windows operating environment, Microsoft DCOM can be configured to use an authentication level of "packet privacy" to encrypt the content of all DCOM network packets or DM .NET Remoting can be configured to send and receive messages over secure HTTP - HTTPS.

2.2.2 Logical Boundaries

This section identifies the security functions that Document 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 security management functions.

2.2.2.1 Security Audit

The components of the Server and Services tier generate logs of actions performed on a document throughout the document's lifecycle. The Desktop provides the user with the interface to review the logs.

2.2.2.2 User data protection

The TOE enforces a role-based access control policy that controls the actions users can perform on documents, based on the roles the user is associated with and the life cycle stage of the document. Users of the TOE are identified and authenticated by the IT environment before any access to the TOE is granted. The TOE defines document management roles, and associates those roles with users and groups that are defined in the IT environment. The roles a user is associated with determine what commands a user can perform. Roles are also associated with the various states in which a document type can exist. The document life cycle defines how the document transitions through its various states. A document life cycle stage is the current state of the document and the transitions that apply to the document in its current state. The TOE ensures the user has an appropriate document management role and that the requested operation is valid for the current life cycle stage of the document before allowing a requested operation to be performed. The Desktop tier and the Server and Services tier work together to implement the role-based access control policy.

The IT environment (specifically, the DB2® Content Manager component of the content repository tier) enforces its own access control policy on the items stored within the content repository, including the items the TOE presents to users as documents. Access to these items is governed by the item's Access Control List (ACL) that identifies the user and the access allowed. The IT environment uses privileges to define what operations a user is allowed to perform on the items. The Library Server component verifies that the user has the required privilege and the ACL associated to the requested item grants access. This access is enforced regardless of the commands a TOE user might be granted by their role assignment. That is, Content Manager access control is always enforced, and Document Manager access control adds another layer of control. Document Manager's role-based access controls cannot grant additional access to Content Manager items, they can only further restrict the access a user is otherwise granted by the Content Manager access controls.

2.2.2.3 Identification

The TOE presents a login screen to users of the Desktop when it is first started. The user identity and password are passed through to the IT environment for identification and authentication prior to granting any further access to the TOE. The TOE enforces the identification and authentication decision received from the IT environment and ensures the user does not gain access to the TOE if identification and authentication fail. The TOE associates the user identity with the current active session and uses this identity and the user's document management roles to enforce the access control policy on documents.

The Desktop client can be configured by the administrator to require the end user to re-login if idle for longer than a configurable interval[4].

The Item Loader component can be run standalone or from the Desktop component. If run standalone, the Item Loader prompts for a user identity and password, which are passed through to the IT environment for identification and authentication prior to granting further access to the functions of the Item Loader. If run from Desktop, then identification and authentication is handled by the Desktop, as described above.

The DM Client API provides two methods whereby a user (i.e., an application invoking DM via the API) can be identified and authenticated: user identity and password; and credential token. The user identity and password mechanism identifies and authenticates the Client API user exactly as the Desktop user is identified and authenticated by the IT environment. A DM credential token is an encrypted string that contains both the user name and the password of the user who is currently logged in from DM Desktop client. DM provides a credential token to plug-in applications launched from DM Desktop client so that these applications may login through the DM Client API without requesting credentials from the user (i.e., without having to prompt again for the username and password that the user already entered at the time he logged into DM Desktop client).

The TOE uses the IBM Crypto for C (also known as ICC Toolkit) cryptomodule, Version 1.4.5, running in FIPS mode, to encrypt login user names and passwords before sending them across the network or saving them, including saving them as part of a credential token for the DM Client API. User names and passwords are encrypted using 128-bit Advanced Encryption Standard (AES) in Cipher Block Chaining (CBC) mode, using a one-time session key. The session key itself is encrypted using a separate key encryption key that is shared by the DM clients and DM Library Server and the encrypted session key and data (user name or password) is then sent over the network or saved as required. The key encryption key and all session keys are generated using the ICC Toolkit.

The ICC Toolkit version 1.4.5 has FIPS 140-2 validation certificate #775 and is listed on the National Institute of Standards and Technology (NIST) web site at http://csrc.nist.gov/cryptval/140-1/1401val2007.htm.

The TOE supports CM's single sign-on functionality, which allows a user to startup the Desktop without having to provide a user name or password (since client authentication is done through CM).

CM must not be configured for single sign-on in the evaluated configuration.

The TOE also supports CM's trusted logon mode. When CM is configured for trusted logon, no password is required. CM assumes the provided user name has already been authenticated and the CM API caller is trusted.

CM must not be configured for trusted logon in the evaluated configuration.

2.2.2.4 Security management

The TOE requires an authorized administrator role to perform the security functions of creating and modifying document management roles, document states, and document classes and defining document life cycle stages. The TOE's authorized administrator security management role is defined in the IT environment.

[4] The TOE also provides a mechanism to lock user accounts if a configured number of consecutive failed login attempts occur. However, the underlying Content Manager system provides a stronger mechanism (since accounts are locked until the authorized administrator unlocks them), so guidance documentation advises using the Content Manager account lock-out mechanism rather than the mechanism provided by the TOE.

2.2.3 Communication Protocols

DM supports two distinct communication protocols for communication between DM components:

- Microsoft Distributed Component Object Model (DCOM)
- Microsoft .NET Remoting

DCOM is the default protocol used. When DM is configured to use DCOM, all DM components use DCOM to communicate. When DM is configured to use .NET Remoting, all DM components use .NET Remoting to communicate. There is no mixed protocol support in which some communications between DM components use one protocol and some use another. For complete details on configuring DM to use DCOM and .NET Remoting, see the DM guidance documentation *Planning and Installing DB2 Document Manager*.

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 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.

3.1 Threats

T.AUDIT	A user may perform unauthorized actions on the TOE that go undetected.
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.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.OS	The operating environments are configured in accordance with the manufacturer's installation guides and in a secure manner that protects them from any unauthorized users or processes and protects the communication between components.
A.PROTECT	The TOE server component will be located within controlled access 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 satisfy assumptions. All of the identified threats and assumptions are addressed under one of the categories below.

4.1 Security Objectives for the TOE

O.AUDIT	The TOE must be able to audit the actions on the controlled items within the TOE.
O.AUTH_SUPPORT	The TOE must enforce the identification and authentication decision made by the IT environment and must provide a mechanism that restricts the scope for unauthorized users to gain logical access to the TOE.
O.MANAGE	The TOE must allow administrators to effectively manage the TOE, and its security functions.
O.OBJ_ACCESS	The TOE must limit access to objects maintained by the TOE to users authorized to access those objects.

4.2 Security Objectives for the IT Environment

OE.PROTECT	The IT environment must ensure that the security functions of the TOE cannot be tampered with or bypassed.
OE.AUTH	The IT environment must ensure that all users are successfully identified and authenticated prior to accessing any TOE resources or data.
OE.TIME	The IT environment shall provide an accurate timestamp.
OE.ACCESS	The IT environment must limit access to the TOE objects maintained by the IT environment to users authorized to access those objects.
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.MANAGE	The IT environment shall provide an authorized administrator role that supports management of the TOE and its security functions, and management of the IT environment.
OE.AUDIT_STORAGE	The IT environment must provide the means to store audit records generated by the TOE and to protect those records from unauthorized modification or deletion.

4.3 Security Objectives for the Environment

OE.ADMIN	Authorized administrators are competent, non-hostile and follow all administrator guidance.

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 the TOE server component is located within controlled access facilities that protect it from unauthorized physical access and modification.

5. IT Security Requirements

This section of the ST specifies the security requirements for the TOE and the IT Environment that will support the TOE. The security requirements comprise both Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs). The SFRs comprise SFRs drawn from the CC Part 2 and an explicitly stated requirement that defines functionality not modeled by the CC. The SARs are drawn only from CC Part 3.

5.1 TOE Security Functional Requirements

The following table identifies the SFRs that are satisfied by IBM DB2® Document Manager, Version 8.4.

Requirement Class	Requirement Component
FAU: Security Audit	FAU_GEN_EX.1: Audit data generation
	FAU_SAR.1: Audit Review
FDP: User data protection	FDP_ACC.1: Complete access control
	FDP_ACF.1a: Security attribute based access control
FIA: Identification and authentication	FIA_ATD.1a: User attribute definition
	FIA_ENF_EX.1: Enforcement of identification and authentication decision
	FIA_UAU.6: Re-authenticating
FMT: Security management	FMT_MSA.1a: Management of security attributes
	FMT_MSA.3a: Static attribute initialization
	FMT_MTD.1a: Management of TSF data
	FMT_MTD.1b: Management of TSF data
	FMT_SMF.1a: Specification of Management Functions

Table 1 TOE Security Functional Components

5.1.1 Security audit (FAU)

5.1.1.1 Audit data generation (FAU_GEN_EX.1)

FAU_GEN_EX.1.1 The TSF shall be able to generate an audit record on the actions that occur during a controlled class item's lifecycle.

FAU_GEN_EX.1.2 The TSF shall record within each audit record at least the following information: Date and time the operation was executed, DM activity, CM subject identity, CM group, the DM role membership, and the additional activity-specific details.

5.1.1.2 Audit Review (FAU_SAR.1)

FAU_SAR.1.1 The TSF shall provide **[authorized users]** with the capability to read **[all 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.

5.1.2 User data protection (FDP)

5.1.2.1 Complete access control (FDP_ACC.1)

FDP_ACC.1.1 The TSF shall enforce the **[DM Access Control SFP]** on **[**

- **subjects: users;**
- **objects: controlled documents;**

- **operations: add; checkout; copy; revise; modify properties; print; transition; view; markup]**.

5.1.2.2 Security attribute based access control (FDP_ACF.1a)

FDP_ACF.1a.1 The TSF shall enforce the **[DM Access Control SFP]** to objects based on the following: **[**
User:
- **identity**
- **groups**
- **document management roles**

Document:
- **life cycle stage]**.

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 User can perform the requested operation on the Document if:
- **The User identity is associated with a document management role that grants the operation for the current life cycle stage of the Document, or**
- **The User identity is included in a group that is associated with a document management role that grants the operation for the current life cycle stage of the Document]**.

FDP_ACF.1a.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **[no additional explicit authorize rules]**.

FDP_ACF.1a.4 The TSF shall explicitly deny access of subjects to objects based on the **[no additional explicit denial 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 users: **[document management roles]**.

5.1.3.2 Enforcement of identification and authentication decision (FIA_ENF_EX.1)

FIA_ENF_EX.1.1 The TSF shall require each environment-defined existing user to be successfully identified and authenticated using support from the IT environment before allowing any other TSF-mediated actions on behalf of that user.

5.1.3.3 Re-authenticating (FIA_UAU.6)

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions **[no user activity via the DM Desktop for administrator-specified period of time]**.

5.1.4 Security management (FMT)

5.1.4.1 Management of security attributes (FMT_MSA.1a)

FMT_MSA.1a.1 The TSF shall enforce the **[DM Access Control SFP]** to restrict the ability to **[*modify*]** the security attributes **[life cycle stage]** to **[authorized administrator]**.

5.1.4.2 Static attribute initialization (FMT_MSA.3a)

FMT_MSA.3a.1 The TSF shall enforce the **[DM Access Control SFP]** to provide **[*[authorized administrator-defined]*]** 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.

5.1.4.3 Management of TSF data (FMT_MTD.1a)

FMT_MTD.1a.1 The TSF shall restrict the ability to **[*create, modify*]** the **[document management roles, states, classes]** to **[authorized administrator]**.

5.1.4.4 Management of TSF data (FMT_MTD.1b)

FMT_MTD.1b.1 The TSF shall restrict the ability to **[*modify*]** the **[session termination parameters]** to **[authorized administrator]**.

5.1.4.5 Specification of Management Functions (FMT_SMF.1a)

FMT_SMF.1a.1 The TSF shall be capable of performing the following security management functions: **[**

- **Create and modify document management roles, states and classes**
- **Define and modify Document life cycle stages**
- **Modify session termination parameters**

].

5.2 IT Environment Security Functional Requirements

The following table identifies the SFRs that are satisfied by the IT environment of IBM DB2® Document Manager, Version 8.4.

Requirement Class	Requirement Component
FAU: Security audit	FAU_STG.1: Protected audit trail storage
FCS: Cryptographic support	FCS_CKM.1: Cryptographic key generation
	FCS_COP.1: Cryptographic operation
FDP: User data protection	FDP_ACC.2: Complete access control
	FDP_ACF.1b: Security attribute based access control
	FDP_ITT.1: Basic internal transfer protection
FIA: Identification and authentication	FIA_AFL.1: Authentication failure handling
	FIA_ATD.1b: User attribute definition
	FIA_UAU.2: User authentication before any action
	FIA_UID.2: User identification before any action
FMT: Security management	FMT_MSA.1b: Management of security attributes
	FMT_MSA.3b: Static attribute initialization
	FMT_MTD.1c: Management of TSF data
	FMT_SMR.1: Security roles
	FMT_SMF.1b: Specification of Management Functions
FPT: Protection of the TSF	FPT_ITC.1: Inter-TSF confidentiality during transmission
	FPT_ITT.1: Basic internal TSF data transfer protection
	FPT_RVM.1: Non-bypassability of the TSP
	FPT_SEP.1: TSF 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.1)

FAU_STG.1.1 The ~~TSF~~ **IT Environment** shall protect the stored audit records from unauthorized deletion.
FAU_STG.1.2 The ~~TSF~~ **IT Environment** shall be able to **[*prevent*]** unauthorized modifications to the stored audit records in the audit trail.

5.2.2 Cryptographic support (FCS)

5.2.2.1 Cryptographic key generation (FCS_CKM.1)

FCS_CKM.1.1 The ~~TSF~~ **IT Environment** shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[Random Number Generation]** and specified cryptographic key sizes **[128 bits]** that meet the following: **[FIPS PUB 186-2]**.

5.2.2.2 Cryptographic operation (FCS_COP.1)

FCS_COP.1.1 The ~~TSF~~ **IT Environment** shall perform **[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 Complete access control (FDP_ACC.2)

FDP_ACC.2.1 The ~~TSF~~ **IT Environment** shall enforce the **[CM Access Control SFP]** on **[Subjects: Users; Objects: Resources]** and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The ~~TSF~~ **IT Environment** shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.

5.2.3.2 Security attribute based access control (FDP_ACF.1b)

FDP_ACF.1b.1 The ~~TSF~~ **IT Environment** shall enforce the **[CM Access Control SFP]** to objects based on the following: **[**

User:

- **Identity**
- **Groups**
- **Privileges**

Resources:

- **ACL]**.

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

The requested operation is allowed if:

1. **If administrative domains have been enabled, the Resource Domain must be PUBLIC or the same as the User Domain AND**
2. **The User's Privileges allow the requested operation to be performed by the User AND**
3. **(The User Privileges include the privilege to bypass ACL checking OR**
4. **Public Access is enabled and the ACL Public Rule grants the requested operation OR**
5. **The ACL includes a rule for the User Name that grants the requested operation OR**
6. **(Public Access is disabled or the ACL Public Rule does not grant the requested operation) and (the ACL does not include a rule for the User Name) and (the ACL includes a rule for a Group assigned to the User that grants the requested operation));**

Otherwise the operation fails].

FDP_ACF.1b.3 The ~~TSF~~ **IT Environment** shall explicitly authorize access of subjects to objects based on the following additional rules: **[no additional explicit authorize rules]**.

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

5.2.3.3 Basic internal transfer protection (FDP_ITT.1)

FDP_ITT.1.1 The ~~TSF~~ **IT Environment** shall enforce the **[DM Access Control SFP, CM 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 Authentication failure handling (FIA_AFL.1)

FIA_AFL.1.1 The ~~TSF~~ **IT Environment** shall detect when **[*an administrator configurable positive integer within [1 – 32767]*]** unsuccessful authentication attempts occur related to **[user logon]**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the ~~TSF~~ **IT Environment** shall **[lock the user account, and ensures it remains locked until unlocked by an authorized administrator]**.

5.2.4.2 User attribute definition (FIA_ATD.1b)

FIA_ATD.1b.1 The ~~TSF~~ **IT Environment** shall maintain the following list of security attributes belonging to individual users: **[identity, group, authentication data, privileges]**.

5.2.4.3 User authentication before any action (FIA_UAU.2)

FIA_UAU.2.1 The ~~TSF~~ **IT Environment** shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.2.4.4 User identification before any action (FIA_UID.2)

FIA_UID.2.1 The ~~TSF~~ **IT Environment** shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

5.2.5 Security management (FMT)

5.2.5.1 Management of security attributes (FMT_MSA.1b)

FMT_MSA.1b.1 The ~~TSF~~ **IT Environment** shall enforce the **[CM Access Control SFP]** to restrict the ability to **[*change_default, query, modify, delete, [*create*]*]** the security attributes **[user identity, groups, privileges]** to **[authorized administrator]**.

5.2.5.2 Static attribute initialization (FMT_MSA.3b)

FMT_MSA.3b.1 The ~~TSF~~ **IT Environment** shall enforce the **[CM Access Control SFP]** to provide **[*[*authorized administrator-defined*]*]** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3b.2 The ~~TSF~~ **IT Environment** shall allow the **[authorized administrator]** to specify alternative initial values to override the default values when an object or information is created.

5.2.5.3 Management of TSF data (FMT_MTD.1c)

FMT_MTD.1c.1 The TSF shall restrict the ability to **[*modify*]** the **[unsuccessful login attempts threshold]** to **[authorized administrator]**.

5.2.5.4 Specification of Management Functions (FMT_SMF.1b)

FMT_SMF.1b.1 The ~~TSF~~ **IT Environment** shall be capable of performing the following security management functions: **[**

- **Management of security attributes used to enforce the CM Access Control SFP;**
- **Management of the unsuccessful login attempts threshold]**.

5.2.5.5 Security roles (FMT_SMR.1)

FMT_SMR.1.1 The ~~TSF~~ **IT Environment** shall maintain the roles **[authorized administrator, authorized non-administrative users]**.

FMT_SMR.1.2 The ~~TSF~~ **IT Environment** shall be able to associate users with roles.

5.2.6 Protection of the TSF (FPT)

5.2.6.1 Inter-TSF confidentiality during transmission (FPT_ITC.1)

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 unauthorized disclosure **and modification** during transmission.

5.2.6.2 Basic internal TSF data transfer protection (FPT_ITT.1)

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.

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

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

5.2.6.4 TSF 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 separation between the security domains of subjects in the TSC.

5.2.6.5 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: Authorisation 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

Requirement Class	Requirement Component
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
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 uthori 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 uthorized 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.

The TOE uses the concept of "classes" to model business processes for managing documents (generically referred to as "items") in the content repository. Distinct document types can be managed using distinct classes. The configuration of a class can be used to model an item's creation, change and approval processes.

There are two types of classes:

- **Controlled classes**—have a change and approval process associated with them. Items assigned to controlled classes fall under a rule-set that is referred to as a life cycle. These rules control who can author the items, who has access to those items when the items are released, and what states are included in that item's life cycle. Life cycle history can also be enabled to track all actions taken on the item, when an action was taken, and by whom. Lifecycle Services processes all items belonging to controlled classes.
- **Stateless classes**—do not follow a change and approval process. Therefore, a life cycle is not required and Lifecycle Services does not process them. Accordingly, states cannot be assigned to stateless classes. This means that documents assigned to a stateless class are not subject to the TOE's access control policy (though they are still subject to the access control policy of the underlying content repository).

6.1 TOE Security Functions

6.1.1 Security Audit

The TOE can be configured to track an item's life cycle activities for items defined in a controlled class.

The following activities can be configured to be logged in the "Lifecycle History" activity log for the items defined in controlled classes:

- Add – Item was created.
- Checkin – Item was checked into the CM library.
- Checkout – Item was checked out from the CM library.
- Copy – Item was copied out from the CM library (that is, a copy was made of the library item, but the item was not checked out).
- Delete – Item was deleted from the CM library.
- Library Update – Item was updated in the CM library (i.e., updates the library with a copy of a checked-out item that is currently being edited. This update will check in a new version and draft of the document, then check it out again)
- Markup added – A new markup item was associated with the item.
- Modify properties – Item properties were modified.
- Notification – An email or instant message notification was sent for the item. Notifications may be requested after other activities have completed like a Rendition, Revise, etc.
- Print – Item has been printed.
- Process – route actions – A user-defined CM doc routing action has been executed on the item from DM. User-defined actions are those actions that are defined as part of the CM document routing process. This only records user-defined doc routing actions executed from within DM.
- Process – system actions – A system-defined CM doc routing action has been executed on the item from DM. System-defined actions include the CM doc routing actions: Change Route, Change Priority, Change

Owner, Terminate Route, Activate and Suspend and the DM doc routing commands Change Details, Select Route and Define Route. This only records system-defined doc routing actions executed from within DM.

- Record Management – A Record Management operation was executed on the item. For example, declaring the item as an item of record. This only records RM operations executed from within DM.
- Rendition – Item has been rendered into another format.
- Revise –Item has been revised. Updates were approved and a new "revision" was created.
- Transition – Item has been transitioned to a different state. (DM Lifecycle)
- View – Item has been viewed.

A number of these activities are associated with controlled operations within the scope of the DM Access Control SFP and can be configured to be logged when users perform controlled operations on controlled documents. The following table associates auditable activities with controlled operations and the Desktop commands that invoke those controlled operations.

Activity	**Controlled Operation**	**Desktop Commands**
Add	Add Items	Add Document, Add Item, Add From Document Template, Add From Library Template
Checkout	Checkout	Checkout, Checkout-Launch
Copy	Copy	Copy
Library Update	Modify Properties	Update Library Item
Markup added	Markup	View
Modify properties	Modify Properties	Modify, Power Modify
Print	Print	Print
Revise	Revise Items	Revise
Transition	Transition	Transition
View	View	View

The following auditable activities are associated with operations that are not controlled within the scope of the DM Access Control SFP:

- Checkin—Maps to the Desktop "Checkin" command. The Checkin operation is not limited by role because a document can be checked-in only by the user that checked it out, and the Checkout operation is a controlled operation
- Delete—Maps to the Desktop "Delete" command. The Delete operation is not limited by role because it is controlled by CM repository security and users therefore have to have appropriate privileges within the scope of the CM Access Control SFP to be able to delete items from a controlled class
- Notification—Notfication actions are performed by the Notification Services service, not by a user in Desktop
- Process – route actions, Process – system actions—These actions map to the Desktop "Manage Routes", "Define Route" and "Select Route" commands. These commands are associated with CM document routing functionality

- Record Management—Maps to the Desktop "Declare Record" command. It is associated with IBM Records Manager functionality
- Rendition—Maps to the Desktop "Rendition" command, but is more typically automated in the state configuration. Regardless, a rendition action does not modify an item's properties and so does not need to be limited by role.

The entries in the activity logs include the following information: Item version; Date and time the operation was executed (the date and time are obtained from the IT environment); activity; additional activity-specific details; user's login name (subject identity); group; and role under which the operation was allowed. Note that the TOE records only activities that actually occur—it does not record failed attempts to perform an activity.

The desktop client provides the command that allows the authorized users to review the log records. The activity logs are stored and protected by the underlying OS of the TOE server component.

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

- FAU_GEN_EX.1: The TOE audits the operations on the item as it goes through its lifecycle within the TOE.
- FAU_SAR.1: The TOE provides the authorized users the interface to review the activity logs.

6.1.2 User data protection

The TOE enforces a role-based access control policy that determines if the user is authorized to perform a requested operation on a controlled document (i.e., a document associated with a controlled class, as described above), based on the user's document management role and the life cycle stage of the document.

A class is used to model an item's creation, change, and approval processes.

The administrator is able to use the classes to create different life cycles for different item types. The administrator defines the states the item type can exist in (e.g., "draft", "approval pending") and specifies the document management roles that can operate on an item in that state. The administrator also defines the manner in which the item transitions from one state to another. This definition is called the Document Lifecycle Map and it is associated with the class. The administrator uses Designer to define classes and Document Lifecycle Maps.

The Document Lifecycle Map defines the set of life cycle stages for the item type associated with the class. Each life cycle stage, in turn, is defined as the current state of the item and the transitions to other states available from the current state. A transition to a new state (and, hence, new life cycle stage) occurs when an operation is performed on the item that causes it to move to the new state.

The actions a user may perform on an item are determined by the document's current life cycle stage (i.e., the document's current state and the transitions available from that state), the document management roles associated with that life cycle stage, and the document management roles with which the user is associated.

The activities that the administrator can assign to a document management role when it is created are: Add Items; Checkout; Copy; Revise Items; Modify Properties; Print; Transition; View; and Markup.

Aspects of the enforcement of the DM Access Control SFP are implemented in each of the three tiers of the TOE architecture. Role-checking is enforced in the Desktop Client tier and in the Server and Services tier. The Content Repository tier checks that the user has the appropriate privileges within the scope of the CM Access Control SFP to perform the requested operation. If the CM Access Control SFP does not permit the user to perform the requested operation on the requested item, the operation will be denied, even if it is allowed by the DM Access Control SFP. By the same token, if the CM Access Control SFP permits the operation on the item, but the TOE has not granted the user access to the operation, the user will not be able to perform the operation on the item.

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

- FDP_ACC.1: The TOE enforces the DM Access Control SFP on users, controlled documents and the following operations that users can perform on controlled documents: add; checkout; copy; revise; modify properties; print; transition; view; and markup.

- FDP_ACF.1a: The TOE enforces the DM Access Control SFP on documents based on the association of that user's identity to document management roles (either directly or through a group) and on the current life cycle stage of the document.

6.1.3 Identification

Users of the TOE and the groups they belong to are defined in the content repository tier of the Document Manager architecture. This tier is in the IT environment of the TOE.

The TOE requires each user of the Desktop to login before granting further access to the capabilities of the TOE. The login information (user identity and password) is passed through to the content repository tier for identification and authentication. The TOE enforces the identification and authentication decision received from the IT environment and ensures the user does not gain access to the TOE via the Desktop if identification and authentication fail. The TOE maintains the association of the user identity with the user's active session and uses this identity to determine the groups the user belongs to, the Desktop template to be displayed to the user, and the document management roles the user is associated with. The TOE uses the role association to determine the operations the user is authorized to perform on documents, and document life cycle stages in which they are authorized to perform those operations.

The Desktop can be configured by the administrator to require the end user to re-authenticate if idle for longer than a configurable interval.

The Item Loader component can be run standalone or from the Desktop component. If run standalone, the Item Loader prompts for a user identity and password, which are passed through to the IT environment for identification and authentication prior to granting further access to the functions of the Item Loader. If run from Desktop, then identification and authentication is handled by the Desktop, as described above.

The DM Client API provides two methods whereby a user (i.e., an application invoking DM via the API) can be identified and authenticated: user identity and password; and credential token.

The user identity and password mechanism identifies and authenticates the Client API user exactly as the Desktop user is identified and authenticated by the IT environment.

A DM credential token is an encrypted string that contains both the user name and the password of the user who is currently logged in from DM Desktop client. DM provides a credential token to plug-in applications launched from DM Desktop client so that these applications may login through the DM Client API without requesting credentials from the user (i.e., without having to prompt again for the username and password that the user already entered at the time he logged into DM Desktop client).

DM plug-in applications (or, simply, plug-ins) are application programs external to DM that can be invoked from DM. Plug-ins are typically customer applications containing customer business logic. They can also be DM Client API applications that login to a DM library. There are two types of plug-ins: client plug-ins and service plug-ins. Client plug-ins are invoked by a DM Desktop command, and service plug-ins are invoked by a service, such as Lifecycle Services. DM Designer is used to configure plug-ins and associate them with Desktop commands, classes and states. Only client plug-ins are passed the credential token, as only client plug-ins have a corresponding DM Desktop client user and password.

When a client plug-in is invoked, DM Desktop client passes to it a data exchange file, which is a Windows temporary .INI file. DM Desktop client generates the data exchange file, including the credential token, at the time it processes execution of the plug-in and deletes the file after the plug-in exits and returns control to DM Desktop client. The credential token is encrypted using the FIPS-conformant ICC toolkit.

The Designer component does not require users to identify or authenticate themselves before accessing its capabilities. By default, Designer is installed on the same computer as the DM Server component. This computer is assumed to be located within a controlled access environment that protects it from unauthorized physical access and modification. In addition, during initial configuration of the TOE, the TOE administrator should use Designer to configure a Desktop template that includes the "Configure" command and that is assigned only to a TOE administrator role. Following the initial configuration of the TOE library and the administrator Desktop template, Designer should always be run via the "Configure" command from this administrator Desktop client. This will ensure that the administrator must be identified and authenticated before accessing other TOE capabilities.

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

- FIA_ATD.1a: The TOE maintains the association of document management roles with users.
- FIA_ENF_EX.1: The TOE enforces the identification and authentication decision made by the content repository tier in the IT environment and ensures the TSF does not provide any access when identification and authentication fail.
- FIA_UAU.6: The TOE requires the user to re-authenticate after an administrator-specified period of inactivity.

The TOE uses the IBM Crypto for C (also known as ICC Toolkit) cryptomodule, Version 1.4.5, running in FIPS mode, to encrypt login user names and passwords before sending them across the network or saving them. User names and passwords are encrypted using 128-bit Advanced Encryption Standard (AES) in Cipher Block Chaining (CBC) mode, using a one-time session key. The session key itself is encrypted using a separate key encryption key that is shared by the DM clients and DM Library Server and the encrypted session key and data (user name or password) is then sent over the network or saved as required. The key encryption key and all session keys are generated using the ICC Toolkit.

The ICC Toolkit version 1.4.5 has FIPS 140-2 validation certificate #775 and is listed on the National Institute of Standards and Technology (NIST) web site at http://csrc.nist.gov/cryptval/140-1/1401val2007.htm.

6.1.4 Security management

The TOE provides the ability to manage its security functions through the Designer, which is the interface through which the administrator can configure and manage the TOE.

The TOE supports a single security management role of administrator. Any user not granted the administrator role that logs into Designer has no ability to perform security management functions and can only view the TOE configuration. Note that a DM administrator is actually a CM administrator—the TOE does not define users or groups but instead relies on the underlying CM repository to manage users and groups, including administrative users. However, no CM interfaces are exposed through DM. A CM administrator must log in separately to CM in order to access CM security management functionality.

Administrators are able to perform the following functions provided by the Designer:

- Create and modify document management roles, including associating users and groups with roles
- Create and modify document states, including associating document management roles with states
- Create and modify classes, including associating Document Lifecycle Templates and states with classes
- Define a document life cycle, including all the states the document can have in the life cycle and the manner in which the document transitions from one state to another
- Define the initial life cycle state that a document will be in when it is first created. This value cannot be overridden
- Modify the parameters used to control the session termination function.

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

- FMT_MSA.1a: The TOE restricts the ability to define how a document will transition from one state to another (i.e., how the document transitions through its life cycle stages) to the administrator.
- FMT_MSA.3a: When a user adds a controlled document to the repository, its initial life cycle stage is the life cycle stage configured as the initial stage when the administrator defined the Document Lifecycle Map for this document type. This value cannot be overridden.
- FMT_MTD.1a: The TOE restricts the ability to create and modify document management roles, states and classes to the authorized administrator.
- FMT_MTD.1b: The TOE restricts the ability to modify session termination parameters to the authorized administrator.

- FMT_SMF.1a: The TOE provides the capability to create and modify document management roles that can then be assigned to users and groups, and document states and classes, and the capability to define document life cycles, which specify the states in which a document can exist, and the manner in which the document transitions from one state to another. The TOE also provides the capability to modify the parameters that control user session timeouts.

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 DB2 Document 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 DB2® Document Manager, Version 8.4 in accordance with the evaluated configuration.

These activities are documented in:

- IBM DB2 Document Manager V8.4 Delivery Operation and Guidance
- IBM DB2 Document Manager Planning and Installing Your Document 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 DB2 Document Manager for Enterprise Edition Version 8.4 Security High-level Functional Specification and Design
- DM 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 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.

These activities are documented in:

- IBM DB2 Document Manager System Administration Guide Version 8 Release 4
- Addendum to the IBM DB2 Document 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 DB2 Document Manager V8.4 Lifecycle document
- IBM DB2 Document Manager V8.4 Flaw Remediation.

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 DB2 Document Manager Version 8.4 FP1 Security Functions Test Plan
- IBM DB2 Document Manager Version 8.4 FP1 Security Functions Test Case.

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 DB2 Document Manager, version 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.

The TOE does not provide any permutational or probabilistic security mechanisms; therefore, no strength of function (SOF) claims is made for the TOE.

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 DB2 Document Manager Version 8.4 Fix Pack 1 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, organizational security policies, and threats are completely covered by security objectives. In addition, each objective counters or addresses at least one assumption, organizational security policy, or threat.

8.1.1 Security Objectives Rationale for the TOE and Environment

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

	T.AUDIT	T.NOAUTH	T.OBJ_ACCESS	A.NOEVIL	A.OS	A.PROTECT
O.AUDIT	X					
O.AUTH_SUPPORT		X				
O.MANAGE		X				
O.OBJ_ACCESS			X			
OE.PROTECT		X	X			
OE.AUTH	X	X	X			
OE.TIME	X					
OE.ACCESS			X			
OE.ADMIN				X		
OE.INSTALL					X	
OE.PHYS						X
OE.TRANSFER					X	
OE.MANAGE		X				
OE.AUDIT_STORAGE	X					

Table 4 Environment to Objective Correspondence

8.1.1.1 T.AUDIT

A user may perform unauthorized actions on the TOE that go undetected.

The Threat is mitigated by ensuring that:

- O.AUDIT: The TOE generates log records of the actions performed on the items controlled by the TOE.
- OE.TIME: The IT environment provides the timestamp used to stamp the log records.
- OE.AUTH: The IT environment ensures that the users of the TOE are identified and authentication, so that the log records will include the user's identity.
- OE.AUDIT_STORAGE: The IT environment provides storage for the audit records generated by the TOE that protects those records from unauthorized modification or deletion.

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 satisfied by ensuring that:

- O.AUTH_SUPPORT: The TOE will provide a mechanism that restricts the scope for unauthorized users to gain logical access to the TOE.
- O.MANAGE: The TOE will only allow administrators to manage the TOE security functions.
- OE.PROTECT: The IT environment will ensure that the TOE cannot be tampered with or bypassed.
- OE.AUTH: The IT environment will ensure that all users are successfully identified and authenticated prior to accessing the TOE and its resources.
- OE.MANAGE: The IT environment defines the authorized administrator role that manages the TOE security functions as well as the IT environment security functions.

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 satisfied by ensuring that:

- 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.
- OE.PROTECT: The IT environment will ensure that the security functions of the TOE cannot be tampered with or bypassed and, therefore, its objects cannot be accessed by unauthorized users.
- OE.AUTH: The IT environment will ensure that all users are successfully identified and authenticated prior to accessing the TOE and its objects.
- OE.ACCESS: The IT environment will ensure that the TOE objects that are maintained in the IT environment can be accessed only by users that are authorized to do so.

8.1.1.4 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, non-hostile and follow all administrator guidance.

8.1.1.5 A.OS

The operating environments are configured in accordance with the manufacturer's installation guides and in a secure manner that protects them from any unauthorized users or processes and protects the communication between components.

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.
- OE.TRANSFER: The IT environment will ensures that the data transmitted between the TOE components is protected from tampering and disclosure.

8.1.1.6 A.PROTECT

The TOE server component will be located within controlled access 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 the TOE is located within controlled access facilities that protect it from unauthorized physical access and modification.

8.2 Security Requirements Rationale

This section provides evidence supporting the internal consistency and completeness of the components (requirements) in the ST. 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.AUTH_SUPPORT	O.MANAGE	O.OBJ_ACCESS	OE.TIME	OE.PROTECT	OE.AUTH	OE.ACCESS	OE.AUDIT_STORAGE	OE.MANAGE	OE.TRANSFER
FAU_GEN_EX.1	X										
FAU_SAR.1	X		X								
FAU_STG.1									X		
FCS_CKM.1							X				
FCS_COP.1							X				
FDP_ACC.1				X							
FDP_ACC.2								X			
FDP_ACF.1a				X							

	O.AUDIT	O.AUTH_SUPPORT	O.MANAGE	O.OBJ_ACCESS	OE.TIME	OE.PROTECT	OE.AUTH	OE.ACCESS	OE.AUDIT_STORAGE	OE.MANAGE	OE.TRANSFER
FDP_ACF.1b								X			
FDP_ITT.1											X
FIA_AFL.1							X				
FIA_ATD.1a				X							
FIA_ATD.1b							X	X			
FIA_ENF_EX.1		X									
FIA_UAU.2							X				
FIA_UAU.6		X									
FIA_UID.2							X				
FMT_MSA.1a			X	X							
FMT_MSA.1b										X	
FMT_MSA.3a			X	X							
FMT_MSA.3b										X	
FMT_MTD.1a			X								
FMT_MTD.1b			X								
FMT_MTD.1c										X	
FMT_SMF.1a			X								
FMT_SMF.1b										X	
FMT_SMR.1										X	
FPT_ITC.1											X
FPT_ITT.1											X
FPT_RVM.1						X					
FPT_SEP.1						X					
FPT_STM.1					X						

Table 5 Objective to Requirement Correspondence

8.2.1.1 O.AUDIT

The TOE must be able to audit the actions on the controlled items within the TOE.

The TOE security objective is satisfied by ensuring that:

- FAU_GEN_EX.1: The TOE generates log records of the actions on the items during its lifecycle within the TOE.
- FAU_SAR.1: The TOE provides the authorized users the ability to review the log records.

8.2.1.2 O.AUTH_SUPPORT

The TOE must enforce the identification and authentication decision made by the IT environment and must provide a mechanism that restricts the scope for unauthorized users to gain logical access to the TOE.

The TOE security objective is satisfied by ensuring that:

- FIA_ENF_EX.1: The TOE enforces the identification and authentication decision received from the IT environment and ensures the user dos not gain access to the TOE if identification and authentication fail.

- FIA_UAU.6: The TOE provides a mechanism that requires a user to re-authenticate to the TOE after an administrator-specified period of inactivity. This restricts the scope of unauthorized users gaining access to the TOE via an unattended user session.

8.2.1.3 O.MANAGE

The TOE must allow administrators to effectively manage the TOE, and its security functions.

This TOE Security Objective is satisfied by ensuring that:

- FAU_SAR.1: The TOE provides the authorized users the ability to review the log records.
- FMT_MSA.1a: The ability to modify the document life cycle stages is restricted to the authorized administrator.
- FMT_MSA.3a: The authorized administrator defines the initial document life cycle stage. This value cannot be overridden when a document is created.
- FMT_MTD.1a: The TOE restricts the ability to create and modify roles to the authorized administrator.
- FMT_MTD.1b: The TOE restricts the ability to modify session termination parameters to the authorized administrator.
- FMT_SMF.1a: The TOE provides the capabilities to create and modify roles, define document life cycles, and modify session termination parameters.

8.2.1.4 O.OBJ_ACCESS

The TOE must limit access to objects maintained by the TOE to users authorized to access those objects.

This TOE Security Objective is satisfied by ensuring that:

- FDP_ACC.1: The TOE enforces the DM Access Control Security Function Policy (SFP) on users, controlled documents, and a specified set of operations that users can perform on those controlled documents.
- FDP_ACF.1a: The TOE enforces the DM Access Control SFP using rules based on the security attributes of the subjects and objects.
- FIA_ATD.1a: The TOE associates users with roles, which are the TOE-managed user attributes on which the DM Access Control SFP bases access control decisions.
- FMT_MSA.1a: The ability to modify the document life cycle stages is restricted to the authorized administrator.
- FMT_MSA.3a: The authorized administrator defines the initial document life cycle stage. This value cannot be overridden when a document is created.

8.2.1.5 OE.PROTECT

The IT environment must ensure that the security functions of the TOE cannot be tampered with or bypassed.

This IT Environment Security Objective is satisfied by ensuring that:

- FPT_RVM.1: The IT environment ensures that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.
- FPT_SEP.1: The IT environment ensures that a security domain is maintained and enforced for execution of the TSF that protects it from interference and tampering by untrusted subjects.

8.2.1.6 OE.AUTH

The IT environment must ensure that all users are successfully identified and authenticated prior to accessing any TOE resources or data.

This IT Environment Security Objective is satisfied by ensuring that:

- FIA_ATD.1b: The IT environment maintains the following security attributes belonging to individual users: user identity, groups, authentication data, and privileges.
- FIA_UAU.2: The IT environment requires each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
- FIA_UID.2: The IT environment requires each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.
- FIA_AFL.1: The IT environment supports this objective by providing an account lockout mechanism that mitigates the threat of a brute-force password guessing attack against the user identification and authentication function.
- FCS_CKM.1, FCS_COP.1: The IT environment provides cryptographic support, through key generation and encryption, to protect user identification and authentication information that is saved by the TOE or transmitted between TOE components.

8.2.1.7 OE.ACCESS

The IT environment must limit access to the TOE objects maintained by the IT environment to users authorized to access those objects.

This IT Environment Security Objective is satisfied by ensuring that:

- FDP_ACC.2: The IT environment enforces the CM Access Control SFP on all subjects and objects defined in the IT environment and the operations among them.
- FDP_ACF.1b: The IT environment enforces the CM Access Control SFP using rules based on the security attributes of the subjects and objects.
- FIA_ATD.1b: The IT environment maintains the following security attributes belonging to individual users: user identity, groups, authentication data, and privileges.

8.2.1.8 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.

8.2.1.9 OE.MANAGE

The IT environment shall provide an authorized administrator role that supports management of the TOE and its security functions, and management of the IT environment.

This IT Environment Security Objective is satisfied by ensuring that:

- FMT_SMR.1: The IT environment defines the authorized administrator role that is able to manage the TOE and its security functions, as well as manage the IT environment.
- FMT_MSA.1b: The IT environment restricts the ability to modify the security attributes that govern the enforcement of the CM Access Control SFP to the authorized administrator.
- FMT_MSA.3b: The authorized administrator defines the initial values of the security attributes that govern the enforcement of the CM Access Control SFP. These values can be overridden by the authorized administrator when an object is created.
- FMT_MTD.1c: The IT environment restricts the ability to modify the unsuccessful login attempts threshold to the authorized administrator.
- FMT_SMF.1b: The IT environment provides the capability to manage the security attributes that govern the enforcement of the CM Access Control SFP and the unsuccessful login attempts threshold.

8.2.1.10 OE.AUDIT_STORAGE

The IT environment must provide the means to store audit records generated by the TOE and to protect those records from unauthorized modification or deletion.

This IT Environment Security Objective is satisfied by ensuring that:

- FAU_STG.1: The IT environment protects stored audit records from unauthorized deletion or modification.

8.3 Security Assurance Requirements Rationale

This ST contains the assurance requirements from the CC EAL3 augmented with ALC_FLR.2 assurance package. The EAL chosen is based on the statement of the security environment (assumptions and threats) 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 govern the assurance required of the TOE. The administrative staff is conscientious, non-hostile and well trained (A.NOEVIL, OE.ADMIN). The TOE is physically protected (OE.PHYS), and properly and securely configured (OE.INSTALL). Given these aspects, a TOE based on good commercial development and maintenance practices is sufficient. EAL3 augmented with ALC_FLR.2 is an appropriate level of assurance for the TOE described in this ST.

8.4 Strength of Functions Rationale

The TOE does not provide any permutational or probabilistic mechanisms; therefore, no SOF claims are made for the TOE.

8.5 Requirement Dependency Rationale

The following table identifies each security functional and assurance 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_EX.1	none	*FPT_STM.1*
FAU_SAR.1	FAU_GEN.1	FAU_GEN_EX.1

ST Requirement	CC Dependencies	ST Dependencies
FAU_STG.1	FAU_GEN.1	FAU_GEN_EX.1
FCS_CKM.1	(FCS_CKM.2 or FCS_COP.1), FCS_CKM.4, FMT_MSA.2	*FCS_COP.1*
FCS_COP.1	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1), FCS_CKM.4, FMT_MSA.2	*FCS_CKM.1*
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1a
FDP_ACC.2	FDP_ACF.1	FDP_ACF.1b
FDP_ACF.1a	FDP_ACC.1 and FMT_MSA.3	FDP_ACC.1 and FMT_MSA.3a
FDP_ACF.1b	FDP_ACC.1 and FMT_MSA.3	***FDP_ACC.2*** and *FMT_MSA.3b*
FDP_ITT.1	(FDP_ACC.1 or FDP_IFC.1)	FDP_ACC.1a
FIA_AFL.1	FIA_UAU.1	***FIA_UAU.2***
FIA_ATD.1a	none	none
FIA_ATD.1b	none	none
FIA_ENF_EX.1	none	***FIA_UID.2, FIA_UAU.2***
FIA_UAU.2	FIA_UID.1	***FIA_UID.2***
FIA_UAU.6	none	none
FIA_UID.2	none	none
FMT_MSA.1a	FMT_SMR.1 and FMT_SMF.1 and (FDP_ACC.1 or FDP_IFC.1)	*FMT_SMR.1* and FMT_SMF.1a and FDP_ACC.1
FMT_MSA.1b	FMT_SMR.1 and FMT_SMF.1 and (FDP_ACC.1 or FDP_IFC.1)	*FMT_SMR.1* and *FMT_SMF.1b* and ***FDP_ACC.2***
FMT_MSA.3a	FMT_MSA.1 and FMT_SMR.1	FMT_MSA.1a and *FMT_SMR.1*
FMT_MSA.3b	FMT_MSA.1 and FMT_SMR.1	*FMT_MSA.1b* and *FMT_SMR.1*
FMT_MTD.1a	FMT_SMF.1 and FMT_SMR.1	FMT_SMF.1a and *FMT_SMR.1*
FMT_MTD.1b	FMT_SMF.1 and FMT_SMR.1	FMT_SMF.1a and *FMT_SMR.1*
FMT_MTD.1c	FMT_SMF.1 and FMT_SMR.1	*FMT_SMF.1b* and *FMT_SMR.1*
FMT_SMF.1a	none	none
FMT_SMF.1b	none	none
FMT_SMR.1	FIA_UID.1	***FIA_UID.2***
FPT_ITC.1	none	none
FPT_ITT.1	none	none
FPT_RVM.1	none	none
FPT_SEP.1	none	none
FPT_STM.1	none	none

Functional components FCS_CKM.1 and FCS_COP.1 have dependencies on FCS_CKM.4 and FMT_MSA.2. The cryptographic module is FIPS 140-2 validated. Therefore, the dependencies of key destruction and secure key values are satisfied by this module's validation as FIPS 140-2 compliant.

8.6 Explicitly Stated Requirements Rationale

The statement of security functional requirements includes explicitly-stated requirements to specify the logging ability of the TOE (FAU_GEN_EX.1) and to specify the ability of the TOE to enforce the identification and authentication decision made by the IT environment.

The logging function of the TOE does not log the enabling and disabling of the function or track the same information in the logs as given in the CC FAU_GEN.1 requirement. However, the FAU_GEN_EXP.1 requirement has a dependency on the IT environment providing the time mechanism used to timestamp the log records.

The TOE does not identify or authenticate users of the TOE—these actions are performed on behalf of the TOE by the IT environment. However, the TOE still has to enforce the identification and authentication decisions rendered by the IT environment and prevent users from accessing TOE functionality until they have been successfully identified and authenticated. This capability has been specified by FIA_ENF_EX.1, which has dependencies on FIA_UID.1 and FIA_UAU.1 for the actual performance of the identification and authentication functions.

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**	**Security management**
FAU_GEN_EXP.1	X			
FAU_SAR.1	X			
FDP_ACC.1		X		
FDP_ACF.1a		X		
FIA_ATD.1a			X	
FIA_ENF_EX.1			X	
FIA_UAU.6			X	
FMT_MSA.1a				X
FMT_MSA.3a				X
FMT_MTD.1a				X
FMT_MTD.1b				X
FMT_SMF.1a				X

Table 6 Security Functions vs. Requirements Mapping

8.8 PP Claims Rationale

See Section 7, Protection Profile Claims.