EMC Documentum

EMC Documentum Content Server™ V5.3

and EMC Documentum Administrator™ V5.3

Security Target V2.0

December 8, 2005

ST prepared by

Suite 5200, 4925 Jones Branch Drive♦McLean, VA 22102-3305♦703 848-0883♦Fax 703 848-0960

TABLE OF CONTENTS

SECTION **PAGE**

Table of Tables and Figures

Table or Figure **Page**

1 Security Target Introduction

1.1 Security Target Identification

TOE Identification: EMC Documentum Content Server version 5.3 (build # 5.3.0.115) and EMC Documentum Administrator version 5.3 (build # 5.3.0.041 with CC update #103292)

ST Title: EMC Documentum Content Server V5.3 and EMC Documentum Administrator V5.3 Security Target

ST Version: Version 2.0

ST Authors: Debra Baker

ST Date: December 8, 2005

Assurance Level: EAL2

Strength of Function: SOF Basic

Keywords: Content Management System, Identification, Authentication, Access Control, Security Target, and Security Management

1.2 Security Target Overview

This Security Target (ST) defines the Information Technology (IT) security requirements for EMC Documentum Content Server Version 5.3. EMC Documentum Content Server is the foundation of EMC Documentum's content management system. EMC Documentum Content Server is the core functionality that allows users to create, capture, manage, deliver, and archive enterprise content. The functionality and features of EMC Documentum Content Server provide content and process management services, security for the content and metadata in the repository, and distributed services. EMC Documentum Content Server provides a full set of content management services, including library services (check in and check out), version control, and archiving options.

1.3 Common Criteria Conformance

The TOE is Part 2 extended, Part 3 conformant, and meets the requirements of Evaluation Assurance Level (EAL) 2 from the Common Criteria Version 2.2 Rev 256 CCIMB-2004-01-001 January 2004.

Interpretations: The following interpretation had a direct impact on the ST.

Table 1-1 Interpretations

Interpretation	Description	Affected Requirements
International Interpretations		
INTERP-137	Rules governing binding should be specifiable	FIA_USB

1.4 Document Organization

The main sections of an ST are the ST Introduction, Target of Evaluation (TOE) Description, TOE Security Environment, Security Objectives, IT Security Requirements, TOE Summary Specification, and Rationale.

Section 2, the TOE Description, describes the product type and the scope and boundaries of the TOE.

Section 3, TOE Security Environment, identifies assumptions about the TOE's intended usage and environment and threats relevant to secure TOE operation.

Section 4, Security Objectives, defines the security objectives for the TOE and its environment.

Section 5, IT Security Requirements, specifies the TOE Security Functional Requirements (SFR), Security Requirements for the IT Environment, and the Security Assurance Requirements.

Section 6, TOE Summary Specification, describes the IT Security Functions and Assurance Measures.

Section 7, Protection Profile (PP) Claims, is not applicable, as this product does not claim conformance to any PP.

Section 8, Rationale, presents evidence that the ST is a complete and cohesive set of requirements and that a conformant TOE would provide an effective set of IT security countermeasures within the security environment. The Rationale has three main parts: Security Objectives Rationale, Security Requirements Rationale, and TOE Summary Specification Rationale.

Section 9 and 10, provide acronym definitions and references.

2 TOE Description

2.1 Product Type

EMC Documentum Content Server is the foundation of EMC Documentum's content management system. EMC Documentum Content Server is the core functionality that allows users to create, capture, manage, deliver, and archive enterprise content data. Content data is the actual data managed by the Content Server. Metadata is the attributes of the data. The functionality and features of EMC Documentum Content Server provide the management and security of content data and metadata in the repository.

2.2 EMC Documentum Content Server Components

The evaluated product consists of the EMC Documentum Content Server, Connection Broker, and EMC Documentum Administrator (Administrator Interface).

2.2.1 EMC Documentum Content Server

Content Management Services

- **Storage and Retrieval**

EMC Documentum Content Server provides a single repository for content and metadata. EMC Documentum Content Server uses an extensible object-oriented model to store content and metadata in the repository. Everything in a repository is stored as objects. The metadata for each object is stored in tables in the underlying RDBMS. Content files associated with an object can be stored in file systems, in the underlying RDBMS, in content-addressed storage systems, or on external storage devices. Content files will be stored in the underlying RDBMS in the evaluated configuration. Content files can be any of a wide variety of formats such as text, graphics, and spreadsheets content.

- **Versioning**

One of the most important functions of a content management system is controlling, managing, and tracking multiple versions of the same document. EMC Documentum Content Server has a powerful set of automatic versioning capabilities to perform those functions. At the heart of its version control capabilities is the concept of version labels. Each document in the repository has an implicit label, assigned by the server, and symbolic labels, typically assigned by the authorized user. EMC Documentum Content Server uses these labels to manage multiple versions of the same document.

- **Data Dictionary**

The data dictionary stores information in the repository about object types and attributes. The information can be used by client applications to apply business rules or provide assistance for users. The data dictionary supports multiple locales, so that much of the information can be localized for the ease of users. When EMC Documentum Content Server is installed, a default set of data dictionary information is set up.

- **Assembly and Publishing**

A feature of both content management and process management services, virtual documents are a way to link individual documents into one larger document. An individual document can belong to multiple virtual documents. When an authorized user changes the individual document, the change

appears in every virtual document that contains that document. An authorized user can assemble any or all of a virtual document's contained documents for publishing or perusal. An authorized user can integrate the assembly and publishing services with popular commercial word processors and publishing tools. The assembly can be dynamically controlled by business rules and data stored in the repository.

Process Management Services

- **Workflows**

EMC Documentum's workflow model allows an authorized user to easily develop process and event-oriented applications for document management. The model supports both production and ad hoc workflows. An authorized user can define workflows for individual documents, folders containing a group of documents, and virtual documents. A workflow's definition can include simple or complex task sequences (including those with dependencies). Users with appropriate permissions can modify in-progress workflows. Workflow and event notifications are automatically issued through standard electronic mail systems while documents remain under secure server control. Workflow definitions are stored in the repository, allowing an authorized user to start multiple workflows based on one workflow definition.

- **Life Cycles**

Many documents within an enterprise have a recognizable life cycle. A document is created, often through a defined process of authoring and review, and then is used and ultimately superseded or discarded. EMC Documentum Content Server's life cycle management services lets an authorized user automate the stages in a document's life. A document's life cycle is defined as a lifecycle and implemented internally as a dm_policy object. The stages in a life cycle are defined in the policy object. For each stage, an authorized user can define prerequisites to be met and actions to be performed before an object can move into the next stage.

2.2.2 Connection Broker

A connection broker is a name server for the EMC Documentum Content Server. When a Connect method is issued, the request goes to a connection broker identified in the client's dmcl.ini file. The connection broker returns the connection information for the repository or particular server identified in the Connect method. The authorized user selects which Content Server to connect to. At that point the EMC Documentum Administrator will connect directly to the chosen Content Server. Connection brokers do not request information from the Content Servers, but rely on the servers to regularly broadcast their connection information to them. Which connection brokers are sent a server's information is configured in the server's server config object. Which connection brokers a client can communicate with is configured in the client's dmcl.ini file. Primary and backup connection brokers in a dmcl.ini file. Doing so ensures that users will rarely encounter a situation in which they cannot obtain a connection to a repository.

2.2.3 Administrator Interfaces

- **EMC Documentum Administrator**

EMC Documentum Administrator allows an authorized administrator to monitor, administer, configure, and maintain the EMC Documentum Content Server and repositories via a Web browser. Authorized administrators can be authenticated via an LDAP server, Operating System user name and password, or Windows domain authentication. The LDAP server and Windows domain authentication methods will not be evaluated.

For example, using EMC Documentum Administrator an authorized administrator can:

- Monitor repository system and resource usage
- Configure a repository
- Create or modify repository users and groups
- Create or modify repository object types
- Create or maintain permission sets (also known as access control lists, or ACLs)
- Create or modify file formats
- Monitor repository sessions
- Run server APIs and issue DQL queries (not evaluated)
- Create or modify storage areas
- Create and run methods and jobs (not evaluated)

2.3 TSF Physical Boundary and Scope of the Evaluation

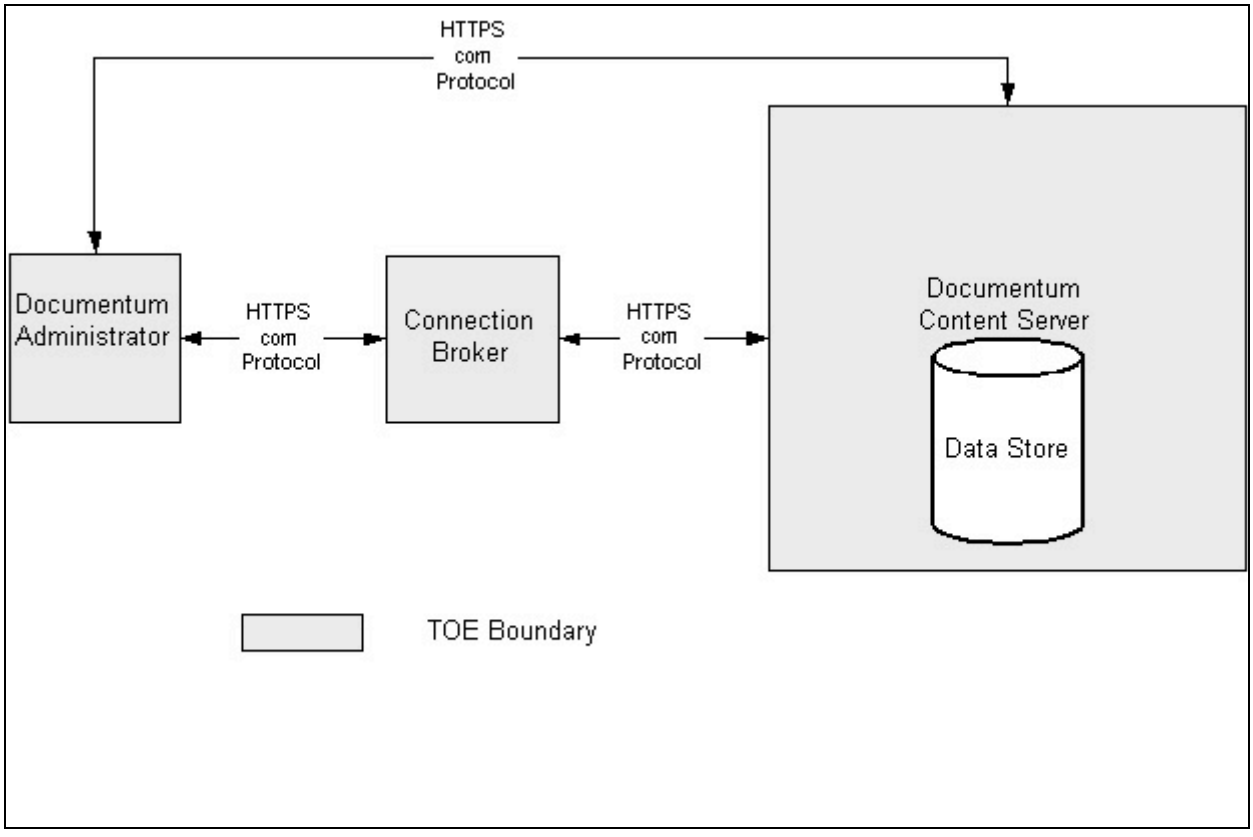

Figure 2-1 TOE Physical Boundary

The TOE includes the following:

- EMC Documentum Content Server V5.3
- Connection Broker;
- EMC Documentum Administrator.

The TOE includes the EMC Documentum Content Server with one repository, Connection Broker, and EMC Documentum Administrator. In the evaluated TOE configuration, repository security will be turned on. The identification and authentication mechanism that will be used in the evaluated configuration is the Operating System username and password. Content files will be stored in the underlying RDBMS in the evaluated configuration.

The evaluated configuration was tested on the following platforms:

EMC Documentum Content Server version 5.3 (build # 5.3.0.115) running on Windows Server 2003 (32 bit Intel Pentium version) with Oracle 10g version 10.1.0.3

Application Server: Tomcat version 5.0.28

EMC Documentum Administrator version 5.3 (build # 5.3.0.041 with CC update #103292) using Internet Explorer running on Microsoft Windows 2003 workstation.

The TOE does not include the following:

- Underlying operating system (OS) software Windows Server 2003 (32 bit Intel Pentium version) and hardware
- Underlying RDBMS: Oracle 10g version 10.1.0.3
- Application Server: Tomcat version 5.0.28
- SSL implementation
- Third party relational database
- Transport standards HTTP, HTTPS, and FTP implementations
- Web Services engine
- Identification and authentication
- User interface

2.4 Logical Boundary

The logical boundary of the TOE will be broken down into the following security class features which are further described in sections 5 and 6. EMC Documentum Content Server provides the following security features:

- **Security audit** - EMC Documentum Content Server provides its own auditing capabilities separate from those of the Operating System. EMC Documentum Content Server provides the ability to search, sort, and view the audit records.
- **User data protection** - EMC Documentum Content Server provides its own complete access control separate from the Operating System between subjects and objects covered by the Content Server User Access Control SFP.

- **Security Management** - EMC Documentum Content Server provides security management through the use of the EMC Documentum Administrator Interface. Through the enforcement of the Content Server User Access Control SFP, the ability to manage various security attributes and TSF data is controlled.
- **Partial Protection of TSF** - EMC Documentum Content Server protects its programs and data from unauthorized access through its own interfaces.

2.5 TOE Security Environment

It is assumed that there will be no untrusted users or software on the EMC Documentum Content Server host. The EMC Documentum Content Server relies upon the underlying operating system (OS) and hardware platform to provide partial protection and execution of the TOE software, disk storage, and reliable time stamps. In addition, the EMC Documentum Content Server relies upon the underlying operating system (OS) and hardware platform to protect the host from other interference or tampering. The OS provides identification and authentication for its own external interfaces. The User Interface is not included in the TOE Boundary.

EMC Documentum Content Server stores metadata in a third party Database Server. EMC Documentum Content Server relies upon third-party SSL software to provide protection of data transfer between TOE components and for a trusted communication path between authorized administrators and the TOE. EMC Documentum Content Server relies on a Web Server to provide web services.

The TOE security environment can be categorized as follows:

- **Cryptographic Support** – All network communications between the EMC Documentum Content Server components are encrypted using SSL. Communications between the EMC Documentum Administrator Interface and the EMC Documentum Content Server host are secure. Since third party software is used to provide confidentiality, the encryption functions are not part of the TOE. The TOE relies on the IT environment to provide cryptographic support. These include:
    - Secure data transfer and trusted communication path between TOE components;
    - With a Trusted Content Services license, the Content Server provides a means of digitally signing the audit trail.
- **Identification and Authentication** - The EMC Documentum Content Server relies on the IT environment to provide authorized administrator and user identification and authentication via the Operating System user name and password.
- **Partial Protection of TSF -** The EMC Documentum Content Server relies on the underlying OS to provide security capabilities for the TOE's protection. For the TOE's own protection the OS includes requirements that relate to the integrity of the TSF. These include SFP domain separation and a reliable time-stamp.

3 TOE Security Environment

This section identifies secure usage assumptions and threats to security. There are no organizational security policies.

3.1 Assumptions

This section contains assumptions regarding the security environment and the intended usage of the TOE.

Table 3-1 Assumptions

1	A.Admin	The authorized administrator is trusted to correctly configure and operate the TOE according to the instructions provided by the TOE documentation.
2	A.Database	The IT environment provides a database to store TSF data.
3	A.NoUntrusted	There are no untrusted users and no untrusted software on the EMC Documentum Content Server host.
4	A.OS	The OS provides file protection and user authentication.
5	A.Physical	The TOE components critical to the security policy enforcement will be protected from unauthorized physical modification by being located within controlled access facilities and behind a Firewall.
6	A.ProtectComm	Those responsible for the TOE will ensure the communications between the EMC Documentum Administrator and EMC Documentum Content Server host are secure.
7	A.Time	The underlying operating system provides reliable time stamps.

Application Notes:

- The Security Policy referenced in A.Physical is referring to the Access Control Policy which is defined in FDP_ACC.2.

- A.ProtectComm provides for a secure communications between the EMC Documentum Administrator and EMC Documentum Content Server host. This can be accomplished by the following:

1. *SSL secure channel between the EMC Documentum Administrator and EMC Documentum Content Server host.*
2. *The User Console is located on the same machine as the EMC Documentum Administrator and EMC Documentum Content Server host.*
3. *There is a direct connection between the EMC Documentum Administrator and EMC Documentum Content Server host on a secure network or via a serial cable or crossover ethernet cable.*

3.2 Threats

The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides. The assumed level of expertise of the attacker for all the threats is unsophisticated, with access to standard equipment and public information.

The TOE must counter the following threats to security:

Table 3-2 Threats

1	T.Abuse	An undetected compromise of the TOE may occur as a result of an authorized user of the TOE (intentionally or otherwise) performing actions the individual is authorized to perform.
2	T.Access	An authorized user of the TOE may access information or resources without having permission from the person who owns, or is responsible for, the information or resource.

3	T.Bypass	An attacker may attempt to bypass TSF security functions to gain unauthorized access to TSF.
4	T.Mismanage	Administrative errors may allow attackers to gain unauthorized access to resources protected by the TOE.
5	T.Privilege	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
6	T.Tamper	An attacker may attempt to modify TSF programs and data.
7	T.Undetect	Attempts by an attacker to violate the security policy may go undetected. If the attacker is successful, TSF data may be lost or altered.

4 Security Objectives

4.1 Security Objectives for the TOE

Table 4-1 Security Objectives for TOE

1	O.Access	The TOE will allow authorized TOE users to access only authorized TOE functions and data.
2	O.Admin	The TOE will provide the functionality to enable an authorized user to effectively manage the TOE and its security functions.
3	O.Attributes	The TOE will be able to maintain user security attributes.
4	O.Audit	The TOE will record audit records for data accesses and use of the system functions.
5	O.NonBypass	The TOE will ensure that the security enforcing functions are invoked and succeed before allowing a TOE function to proceed.
6	O.PartialDomainSep	The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering or unauthorized disclosure, through its own interfaces.
7	O.Roles	The TOE will support multiple administrative roles (see Table 5-3).

4.2 Security Objectives for the Environment

4.2.1 Security Objectives for the IT Environment

The security objectives for the IT environment are as follows:

Table 4-2 Security Objectives for IT Environment

9E	OE.AuditProtect	The IT environment will ensure the protection of the audit storage.
10E	OE.IDAuth	The IT environment will be able to identify and authenticate users prior to allowing access to authorized TOE functions and data.
11E	OE.NonBypass	The IT environment will ensure the security enforcing functions are invoked and succeed before allowing a TOE function to proceed.
12E	OE.PartialDomainSep	The IT environment will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure, through its own interfaces.
13E	OE.Time	The IT environment will provide reliable time stamps.

4.2.2 Non-IT Security Objectives

The Non-IT security objectives are as follows:

Table 4-3 Security Objectives for Non-IT Environment

15N	ON.Install	Those responsible for the TOE will ensure that the TOE is delivered and installed in a manner that maintains IT security.
16N	ON.NoUntrusted	The authorized administrator will ensure that there are no untrusted users and no untrusted software on the EMC Documentum Content Server host.
17N	ON.Operations	The TOE will be managed and operated in a secure manner as outlined in the supplied guidance.
18N	ON.Physical	Those responsible for the TOE will ensure that those parts of the TOE critical to security policy are protected from any physical attack.
19N	ON.ProtectComm	Those responsible for the TOE will protect communications between the EMC Documentum Administrator and EMC Documentum Content Server host.

5 IT Security Requirements

This section provides the TOE security functional and assurance requirements. In addition, the IT environment security functional requirements on which the TOE relies upon are described. These requirements consist of functional components from Part 2 of the CC as well as explicitly stated components derived from Part 2 of the CC, assurance components from Part 3 of the CC, NIAP and International interpretations..

5.1 Conventions

The notation, formatting, and conventions used in this security target (ST) are consistent with version 2.2 of the Common Criteria for Information Technology Security Evaluation. All of the components are taken directly from Part 2 of the CC except the ones noted with "_EXP" in the component name. Font style and clarifying information conventions were developed to aid the reader.

The CC permits four functional component operations: assignment, iteration, refinement, and selection to be performed on functional requirements. These operations are defined in Common Criteria, Part 1, section 4.4.1.3.2 as:

- assignment: allows the specification of an identified parameter;
- refinement: allows the addition of details or the narrowing of requirements;
- selection: allows the specification of one or more elements from a list; and
- iteration: allows a component to be used more than once with varying operations.

This ST indicates which text is affected by each of these operations in the following manner:

- *Assignments* and *Selections* specified by the ST author are in **[*italicized bold text*]**.
- *Refinements* are identified with "**Refinement:**" right after the short name. Additions to the CC text are specified in ***italicized bold and underlined text***.
- *Iterations* are identified with a dash number "-#". These follow the short family name and allow components to be used more than once with varying operations. "*" refers to all iterations of a component.
- *Explicitly Stated Requirements* will be noted with a "_EXP" added to the component name.
- *Application notes* provide additional information for the reader, but do not specify requirements. Application notes are denoted by *italicized text.*
- *NIAP and CCIMB Interpretations* have been reviewed. Relevant Interpretations are included and are noted in Interpretation Notes. Interpretation Notes are denoted by *italicized text.* The original CC text modified by the interpretation is not denoted nor explained.

5.2 TOE Security Functional Requirements

The TOE security functional requirements are listed in Table 5-1.

Table 5-1 Functional Components

No.	Component	Component Name
1	FAU_GEN.1	Audit data generation
2	FAU_GEN.2	User identity association

No.	Component	Component Name
3	FAU_SAR.1	Audit review
4	FAU_SAR.2	Restricted audit review
5	FAU_SAR.3	Selectable audit review
6	FAU_SEL.1	Selective audit
7	FAU_STG_EXP.1-1	Protected audit trail storage
8	FDP_ACC.2	Complete access control
9	FDP_ACF.1	Security attribute based access control
10	FIA_ATD.1	User attribute definition
11	FIA_USB.1	User subject binding
12	FMT_MOF.1	Management of security functions behavior
13	FMT_MSA.1	Management of security attributes
14	FMT_MSA.3	Static attribute initialisation
15	FMT_MTD.1	Management of TSF data
16	FMT_SMF.1	Specification of management functions
17	FMT_SMR.1	Security roles
18	FPT_RVM_EXP.1-1	Non-bypassability of the TSP
19	FPT_SEP_EXP.1-1	TSF domain separation

5.2.1 Class FAU: Security Audit

FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the **[*not specified*]** level of audit; and

c) **[*the following auditable events:***

- ***user login failure,***
- ***all operations performed on objects,***
- ***all operations performed in repository,***
- ***all workflow operations performed,***
- ***all lifecycle operations performed,***
- ***administrative actions performed.*****]**

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST; **[*no additional audit information*]**.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.2 User identity association

Hierarchical to: No other components.

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

Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

FAU_SAR.1 Audit review

Hierarchical to: No other components.

FAU_SAR.1.1 The TSF shall provide **[*Users with Superuser or View Audit privileges*]** with the capability to read **[*all audit information*]** from the audit records.

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

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.2 Restricted audit review

Hierarchical to: No other components.

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

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3 Selectable audit review

Hierarchical to: No other components.

FAU_SAR.3.1 The TSF shall provide the ability to perform **[*searches*]** of audit data based on **[*SysObject-related system events and folder*].**

Dependencies: FAU_SAR.1 Audit review

FAU_SEL.1 Selective audit

Hierarchical to: No other components.

FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

a) **[*event type (event_name) and* object *identity (object_id)*]**

b) **[*lifecycle state (state_name), policy id (policy_id)*]**.

Dependencies: FAU_GEN.1 Audit data generation
FMT_MTD.1 Management of TSF data

Application Note: To stop auditing a system event, use EMC Documentum Administrator or an Unaudit method. A user must have Config Audit privileges to stop auditing by destroying the registry object for an event.

FAU_STG_EXP.1-1 Protected audit trail storage

Hierarchical to: No other components.

FAU_STG_EXP.1.1-1 The TSF shall protect the stored audit records from unauthorised deletion initiated through its own TSFI.

FAU_STG_EXP.1.2-1 The TSF shall be able to ***[prevent]*** unauthorised modifications to the audit records in the audit trail initiated through its own TSFI.

Dependencies: FAU_GEN.1 Audit data generation

Application Note: The TOE makes sure a user has been identified and authenticated before allowing access to the audit trail which is stored in the third party DBMS. To delete audit trail entries a user must have Purge Audit privileges.

5.2.2 Class FDP: User Data Protection

FDP_ACC.2 Complete access control

Hierarchical to: FDP_ACC.1

FDP_ACC.2.1 The TSF shall enforce the **[*Content Server User Access Control SFP*]** on **[*Subjects: process acting on behalf of users and Objects: data, metadata*]** and all operations among subjects and objects covered by the SFP.

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

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1 The TSF shall enforce the **[*Content Server User Access Control SFP*]** to objects based on the following: **[**

Subjects: process acting on behalf of users

Subject Security Attributes:

User Privileges (see Table 6-4)

Extended User Privileges (see Table 6-5)

Roles

Groups

Objects: data, metadata

Object Security Attributes:

Base Object-Level Permissions and Restrictions (see Table 6-6)

Extended Object-Level Permissions and Restrictions (see Table 6-7)**].**

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[**

1. ***A user must be explicitly or implicitly granted explicit or implicit access to a specific object to perform an enumerated set of operations – Browse, Create, Read, Update, Relate, Version, or Delete (See Table 6-6 and Table 6-7)- on that object.***
2. ***A user is explicitly granted object level permissions by association of the user name.***
3. ***A user is implicitly granted object level permissions if he/she belongs to a group which has been granted the permission.***
4. ***Users are granted and restricted access to objects based on object level permissions (base and extended).***

5. ***User privileges define the operations that a user can perform in the repository.***
6. ***The SuperUser role is able to perform all the functions of a user with Sysadmin privileges plus additional functions (see Table 5-3). A user that has SuperUser Privilege has a minimum of Read access to all SysObjects and the ability to modify their own privileges. The SuperUser cannot modify their own extended privileges.***
7. ***Most of the system administration tasks require at least the Sysadmin user privilege. Some, such as deleting audit trail entries, require one of the extended privileges which have to be explicitly assigned. The Sysadmin privilege has full administrative privileges excluding the extended privileges (see Table 5-3 and Table 6-5). The Sysadmin privilege does not override object-level permissions. Sysadmins cannot modify their own extended privileges.***
8. ***A User assigned the privilege level of "None" is able to perform only the actions allowed by the permissions defined at the object level.***
9. ***A User with the privilege of "Create Type" is able to create object types.***
10. ***A User assigned the privilege of "Create Cabinet" is able to create cabinets.***
11. ***A User assigned the privilege of "Create Group" is able to create groups.***
12. ***Basic User privileges (see Table 6-4) do not override object-level permissions and having one of the privileges does not automatically bestow any of the others.***
13. ***Extended User privileges (see Table 6-5) are not hierarchical. For example, granting a user Purge Audit privilege does not confer Config Audit privilege also.***
14. ***User privileges do not override object-level permissions when repository security is turned on. The security_mode attribute in the docbase config object controls whether object-level security is imposed on the Repository.***
15. ***Object-level permissions are defined as entries in ACL objects. Each SysObject (or SysObject subtype) object has an associated ACL. The entries in the ACL identify users and groups and define their object-level permissions to the object with which the ACL is associated.***
16. ***Table Permits further refine access at the RDBMS table (see Table 6-8).*** **]**.

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[*no additional rules*]**.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following rules: **[*no additional rules*]**.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

5.2.3 Class FIA: Identification and Authentication

FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

- **[*User identity,***
- ***User State (active/inactive),***
- ***Default Permission Set (A permission set to use to assign the default permissions to objects created by a user).***
- ***Groups***
- ***User Privileges (See Table 6-4),***
- ***Extended User Privileges (See Table 6-5),***
- ***Roles (Superuser, Sysadmin, User with Create Group, User with Create Cabinet, User with Create Type and User),***
- ***Turn off authentication failure checking*]**.

Dependencies: No dependencies.

Application Note: Turn off authentication failure checking - If checked, user may exceed the number of failed logins specified in the Maximum Authentication Attempts field of the docbase config object.

FIA_USB.1 User-subject binding

Hierarchical to: No other components.

FIA_USB.1.1: The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: **[*User identity, User State (active/inactive), Default Permission Set, Groups, User Privileges, Extended User Privileges, Roles, and Turn off authentication failure checking*]**.

FIA_USB.1.2: The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: **[*none*]**.

FIA_USB.1.3: The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: **[*none*]**.

Dependencies: FIA_ATD.1 User attribute definition

Interpretation Note: CCIMB #137 updates FIA_USB.1

5.2.4 Class FMT: Security Management (FMT)

FMT_MOF.1 Management of Security Functions Behavior

Hierarchical to: No other components.

FMT_MOF.1.1 The TSF shall restrict the ability to **[*determine the behavior of, disable, enable, and modify the behavior of*]** the functions **[*related to the selection of which events are to be audited (see FAU_SEL.1.1) and audit (see FAU_GEN.1.1)*]** to **[*User with Config Audit Privileges*].**

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of management functions (CCIMB 065)

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1 The TSF shall enforce the **[*Content Server User Access Control SFP*]** to restrict the ability to **[*query, modify, delete,* [*and other operations as specified in Table 5-2*]** the security attributes **[*as specified in Table 5-2*]** to **[*the role as specified in Table 5-2*]**.

Dependencies: [FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions (CCIMB 065)

Table 5-2 Management of Security Attributes

Subjects with roles of the following:	Allowed Action on Specified Security Attributes
Superuser	• Query, create, alter, and drop user identity • Query, set a user state to be active/inactive • Query, set a user source (on initial set up of user account, the superuser configures the way that the user will authenticate) • Query, set default folder of user • Query, set default permission set of user • Query, set default group of user • Query, create, modify, reassign, and delete roles; assign users to roles • Query, create, alter, and drop groups; assign users, roles, and groups to a group; remove users from group • Query, set user privileges and extended privileges • Query, set *turn off authentication failure handling* • Query, set base object-level and extended object-level permissions
Sysadmin	• Query, create, alter, and drop user identity • Query, set a user state to be active/inactive • Query, set a user source (on initial set up of user account, the sysadmin configures the way that the user will authenticate) • Query, set default folder of user • Query, set default permission set of user • Query, set default group of user • Query, create, modify, reassign, and delete roles; assign users to roles • Query, create, alter, and drop groups; assign users, roles, and groups to a group; remove users from group • Query, set user privileges and extended privileges • Query, set *turn off authentication failure handling*
User with Create Group	Query, create, modify, and delete own groups; assign users, roles, and groups to own group; remove users from own group
User with Create Cabinet	Query users and groups
User with Create Type	Query users and groups
User	Query users and groups

FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

FMT_MSA.3.1 The TSF shall enforce the **[*Content Server User Access Control SFP*]** to provide **[*restrictive*]** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the **[*Superuser, Sysadmin, and User with Create Group Privileges*]** to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1 The TSF shall restrict the ability to **[*query, modify, delete,* [*create*]] *as specified in Table 5-3*]** the **[*TSF Data as specified in Table 5-3*]** to **[*the role as specified in Table 5-3*].**

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of management functions (CCIMB 065)

Table 5-3 Management of TSF Data

Role	Description	Allowed Operations on TSF Data (Management Functions)
Superuser	User has superuser privileges (The SuperUser is able to Perform all the functions of a user with Sysadmin privileges plus additional functions. The Superuser privilege gives a user a minimum of Read access to all SysObjects and the ability to change their object-level permissions.)	The Superuser can: • Query, create, alter, and drop user identity • Query, create, modify, reassign, and delete roles; assign users to roles • Query, create, alter, and drop groups; assign users, roles, and groups to a group; remove users from group • Create, modify, and delete system-level ACLs • Grant and revoke Create Type, Create Cabinet, and Create Group privileges • Configure and review audit logs • Query, set user privileges and extended privileges • Unlock objects in the repository • Modify or remove another user's groups or private ACLs • Create, modify, or remove system ACLs • Grant and revoke Superuser and Sysadmin privileges • Grant and revoke Config Audit, Purge Audit, and View Audit privileges for all users except superusers • View audit trail entries

Role	Description	Allowed Operations on TSF Data (Management Functions)
Sysadmin	User has system administration privileges (The Sysadmin privilege does not override object-level permissions.)	• Query, create, alter, and drop user identity • Query, create, modify, reassign, and delete roles; assign users to roles • Query, create, alter, and drop groups; assign users, roles, and groups to a group; remove users from group • Create, modify, and delete system-level ACLs • Grant and revoke Create Type, Create Cabinet, and Create Group privileges • Create, modify, and delete system-level ACLs • Query, set user privileges and extended privileges
User with Create Group	User can create groups	• Query, create, modify, and delete groups; assign users, roles, and groups to a group; remove users from group
User with Create Cabinet	User can create cabinets	None
User with Create Type	User can create object types	None
User	User has no special privileges	None

Application Note: The user privileges are additive, not hierarchical. For example, granting Create Group to a user does not give the user Create Cabinet or Create Type privileges. If an authorized administrator wants a user to have both privileges, the authorized administrator must explicitly give them both privileges. Typically, the majority of users in a repository have None as their privilege level. Some users, depending on their job function, will have one or more of the higher privileges. A few users will have either Sysadmin or Superuser privileges. User privileges do not override object-level permissions when repository security is turned on. However, a superuser always has at least Read permission on any object and can change the object-level permissions assigned to any object. Applications and methods that are executed with Content Server as the user always have Superuser privileges.

Customized roles can be created.

FMT_SMF.1 Specification of management functions

Hierarchical to: No other components.

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

- ***determine the behavior of, disable, enable, and modify the behavior of the functions related to the selection of which events are to be audited (see FAU_SEL.1.1) and audit (see FAU_GEN.1.1) (see FMT_MOF.1),***
- ***query, modify, delete, create, and other operations on the security attributes as specified in Table 5-2 (see FMT_MSA.1),***
- ***query, modify, delete, create as specified in*** Table 5-3 ***the TSF Data as specified in*** Table 5-3 ***(See FMT_MTD.1)*****].**

Dependencies: No Dependencies

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1 The TSF shall maintain the roles **[*Superuser, Sysadmin, User with Create Group, User with Create Cabinet, User with Create Type, and User*].**

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

Dependencies: FIA_UID.1 Timing of identification

5.2.5 Class FPT: Protection of the TOE Security Functions

FPT_RVM_EXP.1-1 Non-bypassability of the TSP

Hierarchical to: No other components.

FPT_RVM_EXP.1.1-1 The TSF, when invoked by the underlying host OS, shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Dependencies: No dependencies.

FPT_SEP_ EXP.1-1 TSF domain separation

Hierarchical to: No other components.

FPT_SEP_ EXP.1.1-1 The TSF, when invoked by the underlying host OS, shall maintain a security domain that protects it from interference and tampering by untrusted subjects in the TSC.

FPT_SEP_ EXP.1.2-1 The TSF, when invoked by the underlying host OS, shall enforce separation between the security domains of subjects in the TSC.

Dependencies: No dependencies.

Application Note: The EMC Documentum Content Server makes certain the user has been identified and authenticated before allowing access to the TSF Data.

5.2.6 Strength of Function

The overall strength of function requirement is SOF-Basic. Since FIA_UAU.2 is in the IT Environment, there is not a specific SOF claim.

5.3 Security requirements for the IT Environment

EMC Documentum Content Server requires that the operating system platform provide reliable time stamps. EMC Documentum Content Server requires that the operating system provides TSF domain separation. Since third party software is used to provide confidentiality, the encryption functions are not part of the TOE.

Table 5-4 Functional Components for the IT environment

No.	Component	Component Name
20	FAU_STG_EXP.1*	Protected audit trail storage
21	FIA_UAU.2	User authentication before any action
22	FIA_UID.2	User identification before any action
23	FPT_RVM_EXP.1-2	Non-bypassability of the TSP
24	FPT_SEP_EXP.1-2	TSF domain separation
25	FPT_STM.1	Reliable time stamps

5.3.1 Class FAU: Security Audit

FAU_STG_EXP.1-2 Protected audit trail storage

Hierarchical to: No other components.

FAU_STG_EXP.1.1-2 The IT environment shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG_EXP.1.2-2 The IT environment shall be able to prevent unauthorised modifications to the audit records in the audit trail.

Dependencies: FAU_GEN.1 Audit data generation

Application Note: The TOE makes sure a user has been identified and authenticated before allowing access to the audit trail which is stored in the third party DBMS. To delete audit trail entries a user must have Purge Audit privileges. The TOE relies on the underlying OS, DBMS, and hardware to protect the audit trail storage.

5.3.2 Class FIA: Identification and Authentication

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1

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

Dependencies: FIA_UID.1 Timing of identification

Application Note: When a user or application attempts to open a repository connection or reestablish a timed out connection, Content Server immediately authenticates the user account. The server checks that the user is a valid, active repository user. If not, the connection is not allowed. If the user is a valid, active repository user, Content Server then authenticates the user name and password. The EMC Documentum Administrator Interface and Content Server require each user to be successfully authenticated. Authentication is provided by the Operating System. The Content Server and EMC Documentum Administrator Interface will honor what the OS has authenticated.

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1

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

Dependencies: No dependencies.

Application Note: The EMC Documentum Administrator Interface and Content Server require each user to be successfully identified. Identification is provided by the Operating System. The Content Server and EMC Documentum Administrator Interface will honor what the OS has identified.

5.3.3 Class FPT: Protection of the TOE Security Functions

FPT_RVM_EXP.1-2 Non-bypassability of the TSP

FPT_RVM_EXP.1.1-2: The security functions of the host OS shall ensure that host OS security policy enforcement functions are invoked and succeed before each function within the scope of control of the host OS is allowed to proceed.

Dependencies: No dependencies.

FPT_SEP_EXP.1-2 TSF domain separation

Hierarchical to: No other components.

FPT_SEP_EXP1.1-2 The security functions of the host OS shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects in the scope of control of the host OS**.**

FPT_SEP_EXP.1.2-2 The security functions of the host OS shall enforce separation between the security domains of subjects in the scope of control of the host OS.

Dependencies: No dependencies

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

FPT_STM.1.1 **Refinement:** The ***IT environment*** shall be able to provide reliable time stamps for its own use.

Dependencies: No dependencies

5.4 TOE Security Assurance Requirements

The Security Assurance Requirements for the TOE are the assurance components of Evaluation Assurance Level 2 (EAL2) taken from Part 3 of the Common Criteria. None of the assurance components are refined. The assurance components are listed in Table 5-5 below.

Table 5-5 EAL2 Assurance Components

Item	Component	Component Title
1	ACM_CAP.2	Configuration items
2	ADO_DEL.1	Delivery procedures
3	ADO_IGS.1	Installation, generation, and start-up procedures
4	ADV_FSP.1	Informal functional specification
5	ADV_HLD.1	Descriptive high-level design
6	ADV_RCR.1	Informal correspondence demonstration
7	AGD_ADM.1	Administrator guidance
8	AGD_USR.1	User guidance

Item	Component	Component Title
9	ATE_COV.1	Evidence of coverage
10	ATE_FUN.1	Functional testing
11	ATE_IND.2	Independent testing – sample
12	AVA_SOF.1	Strength of TOE security function evaluation
13	AVA_VLA.1	Developer vulnerability analysis

Further information on these assurance components can be found in the Common Criteria for Information Technology Security Evaluation (CCITSE) Part 3.

6 TOE Summary Specification

6.1 IT Security Functions

6.1.1 Overview

Section 6 describes the specific security functions that meet the criteria of the security class features that are described in section 2.4. The following sections describe the IT Security Functions of the EMC Documentum Content Server interface and the EMC Documentum Administrator interface. Together these two interfaces provide the security functions which satisfy the TOE security functional requirements. This section includes a bi-directional mapping between functions and requirements that clearly shows which functions satisfy which requirements and that all requirements are met. In section 6, the EMC Documentum Content Server interface and the EMC Documentum Administrator interface will be mutually referred to as EMC Documentum Content Server.

Table 6-1 Security Functional Requirements mapped to Security Functions

Item	SFRs	Security Class	Security Functions	Sub-functions
1	FAU_GEN.1	Security audit	Security Audit	SA-1
2	FAU_GEN.2	Security audit	Security Audit	SA-2
3	FAU_SAR.1	Security audit	Security Audit	SA-3
4	FAU_SAR.2	Security audit	Security Audit	SA-4
5	FAU_SAR.3	Security audit	Security Audit	SA-5
6	FAU_SEL.1	Security audit	Security Audit	SA-6
7	FAU_STG_EXP.1-1	Security audit	Security Audit	SA-7
8	FDP_ACC.2	User data protection	Manage User Access	MUA-1
9	FDP_ACF.1	User data protection	Manage User Access	MUA-1
10	FIA_ATD.1	Identification and Authentication	Manage User Access	MUA-2
11	FIA_USB.1	User subject binding	Manage User Access	MUA-3
12	FMT_MOF.1	Security management	Security Management	SM-1
13	FMT_MSA.1	Security management	Security Management	SM-2
14	FMT_MSA.3	Security management	Security Management	SM-3
15	FMT_MTD.1	Security management	Security Management	SM-4
16	FMT_SMF.1	Security management	Security Management	SM-5
17	FMT_SMR.1	Security management	Security Management	SM-6
18	FPT_RVM_EXP.1-1	Protection of the TSF	Manage User Access	MUA-4
19	FPT_SEP_EXP.1-1	Protection of the TSF	Manage User Access	MUA-5

6.1.2 Security Audit Function

SA-1 Audit trail (FAU_GEN.1)

Auditing is a security feature that allows an authorized user to monitor events that occur in a repository. Events are operations performed on objects in a repository or something that happens in an application. Auditing an event creates an audit trail, a history in the repository of the

occurence of the event. The Content Server updates system event audit data which is then stored in the third party DBMS. System events are events that Content Server recognizes and can audit automatically. For example, checking in a document can be an audited system event. A list of auditable security relevant system events is in Table 6-3.

An authorized administrator can also use the information in an audit trail to:

- Analyze patterns of access to objects
- Monitor when critical documents change or when the status of a critical document changes
- Monitor the activity of specific users

There are many ways to conduct auditing. For example, an authorized user can audit:

- All occurrences of a particular event on a given object or given object type
- All occurrences of a particular event in the repository, regardless of the object to which it occurs
- All workflow-related events in the repository
- All occurrences of a particular workflow event for all workflows started from a given process definition
- All executions of a particular job
- All events in the repository

Depending on the particular event and its target, an authorized user can also choose to audit an event only when the target is controlled by a particular application, attached to a particular lifecycle, or in a particular state in a particular lifecycle.

An audit trail is the history of an audited event. Each occurence of an audited event is recorded in one entry in an audit trail. Audit trail entries are stored in the repository as persistent objects. Depending on the event, the objects are dm_audittrail, dm_audittrail_acl, or dm_audittrail_group objects. Audit trail entries store pertinent information about the events, such as when the events occurred, what objects were involved, and who performed the actions.

Table 6-2 Default Auditable Events

The Content Server audits the events in Table 6-2 by default.

Auditable event	Event names
all executions of an audit or unaudit method	dm_audit and dm_unaudit
removal of an audit trail entry from the repository	dm_purgeaudit PURGE_AUDIT
user login failure	dm_logon_failure

Table 6-3 System Auditable Events

The auditing of system events is configurable by an authorized user. To initiate auditing of a system event, an authorized user must have Config Audit privileges. Initiating auditing for a system event creates a dmi_registry object that records the event's registration for auditing.

Auditable event	Targeted object type	Event names
All auditable events in repository	0 or omitted	dm_all (or all)
Any event on any Sysobject or the	dm_sysobject	

Auditable event	Targeted object type	Event names
specified Sysobject		
Assume User	dm_user	dm_assume
Execution of Audit method.	all object types	dm_audit
Authenticate User	dm_user	dm_authenticate
Logon	dm_user	dm_connect
Destroy Object	dm_sysobject dm_acl dm_user dm_group	dm_destroy
Logoff	dm_user	dm_disconnect
Fetch Object	dm_sysobject	dm_fetch
Install	dm_policy dm_process dm_activity	dm_install
Kill Session	not applicable	dm_kill
Logon Failure	dm_user	dm_logon_failure
Purge Audit	dm_audittrail dm_audittrail_acl dm_audittrail_group	dm_purgeaudit
Save Object	dm_sysobject dm_acl dm_group dm_user	dm_save
Copy Object	dm_sysobject dm_acl	dm_saveasnew
Unaudit Event	all object types	dm_unaudit
Uninstall	dm_policy dm_process dm_activity	dm_uninstall

SA-2 User identity association (FAU_GEN.2)

The Content Server is able to associate each auditable event with the identity of the user that caused the event. Audit trail entries store pertinent information about the events, such as when the events occurred, what objects were involved, and who performed the actions.

SA-3 Audit review (FAU_SAR.1)

Authorized users are able to view the audit trail via the EMC Documentum Administrator. What can be viewed is determined by the user's privileges and the value in an audit trail entry's i_audited_obj_class attribute. Users with Superuser or View Audit privileges can view any audit trail entry.

SA-4 Restricted audit review (FAU_SAR.2)

The TSF prohibits all users read access to the audit records, except those users that have been granted explicit read-access. Unauthorized users are not able to read the audit records in the audit trail. As described in SA-3, only Users with Superuser or View Audit privileges can view any audit trail entry. Users without Superuser or View Audit privileges can view audit trail entries for SysObject-related system events if they have at least Browse privileges for the audited object. Users without Superuser or View Audit privileges cannot view audit trail entries for ACL, group, and

user-related events. Users who are the owner of an audited object can always view audit trail entries for the object.

SA-5 Selectable audit review (FAU_SAR.3)

The TSF provides the ability to perform searching of audit data based on SysObject-related system events and folder. The audit trail objects are returned is subject to the same restrictions as those imposed for viewing audit trail entries through EMC Documentum Administrator, with one exception. A user must have Superuser or View Audit privileges to query or retrieve objects of type dmi_audittrail_attrs. If a user does not have either of those privileges and wants to retrieve all audited attribute values for a particular event, including any stored in a dmi_audittrail_attrs object, query the computed attribute, attribute_list_values.

SA-6 Selective audit (FAU_SEL.1)

The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

- event type (event_name) and object identity (object_id)
- lifecycle state (state_name), policy id (policy_id).

An authorized user is able to configure which system events are audited. System events are associated with lifecycles, workflows, and jobs. Refer to Table 6-3 for a list of recognized system events. To initiate auditing of a system event, an authorized user must have Config Audit privileges. When an audited system event occurs, Content Server automatically generates the audit trail entry.

Event_name - Defines the event to stop auditing.

Object id - Identifies the particular object or object type for which the event is being audited.

Policy id - Identifies a lifecycle.

State_name - Identifies a particular state in the lifecycle identified in *policy_id*.

SA-7 Protected audit trail storage (FAU_STG_EXP.1-1)

The TSF protects the stored audit records in the audit trail from unauthorised deletion. The TSF is able to prevent unauthorised modifications to the audit records in the audit trail. The TOE makes sure a user has been identified and authenticated before allowing access to the audit trail which is stored in the third party DBMS. To delete audit trail entries a user must have Purge Audit privileges.

6.1.3 Manage User Access Function

MUA-1 Access control function (FDP_ACC.2) (FDP_ACF.1)

The Content Server User Access Control Security Functional Policy controls authorized user access to objects within the TOE's Scope of Control. The Content Server supports a set of user privileges, object-level permissions, and table permits that determine what operations a user can perform on a particular object.

User privileges are always enforced whether repository security is turned on or not. Object-level permissions and table permits are only enforced when repository security is on. In the evaluated TOE configuration, repository security will be turned on.

The Content Server allows access and denies access based on User and Extended Privileges as well as roles and groups that the authorized user is assigned. In addition, the Content Server

allows and restricts access at the object level (data, metadata) based on ACLs defined by Base Object-Level Permissions and Restrictions and Extended Object-Level Permissions and Restrictions. To further refine access control, table permits are defined that control access to the RDBMS tables represented by registered tables in the repository.

At the lowest level, the subjects are processes acting on behalf of authorized users. At the highest level, the subjects are authorized users that have been assigned authorized roles (Superuser, Sysadmin, and User). These authorized users are allowed access based on the subject security attributes: User Privileges, Extended Privileges, Roles, and Groups. In addition, access is allowed or denied based on object level security attributes (Base Object-Level Permissions and Restrictions and Extended Object-Level Permissions and Restrictions). The User Privileges and Object-Level Permissions are further described in detail below.

User Privileges

User privileges define what administrative operations a user can perform in a repository. Table 6-4 describes the basic user privileges that may be assigned to users. User privileges map to user roles in Common Criteria terminology.

Table 6-4 User Privileges

There are six basic levels of user privileges listed in the below table 6-4.

Privilege	Description
None	User has no special privileges
Create Type	User can create object types
Create Cabinet	User can create cabinets
Create Group	User can create groups
Sysadmin	User has system administration privileges
Superuser	User has superuser privileges

The None privilege allows a user to perform only the actions allowed by the permissions defined at the object level. Typically, the majority of repository users have the None privilege. The Create Type, Create Group, or Create Cabinet privileges allow a user to create the item identified by the privilege name. These privileges do not override object-level permissions and having one of the privileges does not automatically bestow any of the others. For example, a user may have the privilege to create cabinets but not object types. Another user may have only the privilege to create groups. A user who creates an object type, group, or cabinet is the owner of the item and can also modify or remove it.

Sysadmin privileges allow a user to:

- Create, alter, and drop users and groups
- Create, modify, and delete system-level ACLs
- Grant and revoke Create Type, Create Cabinet, and Create Group privileges
- Create types, cabinets, and printers
- Manipulate workflows or work items, regardless of ownership
- Manage any object's lifecycle
- Set the a_full_text attribute

- The Sysadmin privilege does not override object-level permissions.

Superuser privilege allows a user to:

- Perform all the functions of a user with Sysadmin privileges
- Unlock objects in the repository
- Modify or drop another user's user-defined object type
- Create subtypes that have no supertype
- Register and unregister another user's tables
- Select from any underlying RDBMS table regardless of whether it is registered or not
- Modify or remove another user's groups or private ACLs
- Create, modify,or remove system ACLs
- Grant and revoke Superuser and Sysadmin privileges
- Grant and revoke Config Audit, Purge Audit, and View Audit privileges
- View audit trail entries

The Superuser privilege gives a user a minimum of Read access to all SysObjects and the ability to change their object-level permissions.

Table 6-5 Extended User Privileges

There are three extended user privileges as seen in Table 6-5.

Privilege	Description
Config audit	The user can configure auditing.
Purge audit	The user can purge existing audit trails.
View Audit	User can view audit trail entries.

The extended user privileges are not hierarchical. For example, granting a user Purge Audit privilege does not confer Config Audit privilege also. Repository owners, superusers, and users with the View Audit permission can view all audit trail entries. Other users in a repository can view only those audit trail entries that record information about objects other than ACLs, groups, and users. Only repository owners and Superusers may grant and revoke extended user privileges, but they may not grant or revoke these privileges for themselves.

Object Level Permissions

The Object Level Permissions allows an authorized user to use ACLs to further define access to objects. Object-level permissions are access permissions assigned to every SysObject (and SysObject subtype) in the repository.

An access control entry may be one of the following types:

- AccessPermit
- ExtendedPermit
- AccessRestriction
- ExtendedRestriction

- RequiredGroup
- RequiredGroupSet

An entry's permit type is recorded in the r_permit_type attribute in the ACL object. This attribute stores an integer value that represents the type of the entry.

Note: AccessPermit and ExtendedPermit permits for a given user or goup are always stored in the same entry. The permit_type for that entry is set to the integer value representing AccessPermit. Similarly, AccessRestriction and ExtendedRestriction permits for a given user or group are always stored in the same entry, and the permit_type for that entry is set to the integer value representing AccessRestriction.

Note: ApplicationPermit and ApplicationRestriction entries are not recognized by the Content Server. These permission levels are only enforced by the user applications. Since the user applications are outside the scope of the TOE Boundary, ApplicationPermit and ApplicationRestriction entries are not included as part of the Content Server User Access Control SFP.

The following sections describe each entry type.

AccessPermit and ExtendedPermit Entries

An AccessPermit entry defines a base object-level permission for a user or group. The base object-level permissions are None, Browse, Read, Relate, Version, Write, and Delete (See Table 6-4 below).

An ExtendedPermit entry defines an extended object-level permission for a user or group. The extended object-level permissions are: change_location, change_owner, change_state, change_permit, delete_object, and execute_proc (See Table 6-7 below).

In the ACL, both access permits and extended permits are stored in the same entry, whose permit_type is set to AccessPermit. However, when an authorized user grants or revokes these permits, the authorized user must specify whether the AccessPermit or ExtendedPermit are being granted or revoked. This is specified by defining PERMIT_TYPE as either AccessPermit, ExtendedPermit, AccessRestriction, or Extended Restriction and then specifying the PERMIT_LEVEL.

Table 6-6 Base Object-Level Permissions and Restrictions

Note: Whether the authorized user is setting this as a Permission or Restriction is specified by defining the PERMIT_TYPE.

Permission/Restriction	Level	Description
None	1	No access is permitted
Browse	2	The user can look at attribute values but not at associated content.
Read	3	The user can read content but not update.
Relate	4	The user can attach an annotation to the object.
Version	5	The user can version the object.
Write	6	The user can write and update the object.
Delete	7	The user can delete the object.

These Base Object-level permissions are hierarchical. For example, a user with Version permission also has the access accompanying Read and Browse permissions. Or, a user with Write permission also has the access accompanying Version permission.

Table 6-7 Extended Object-Level Permissions and Restrictions

Permission/Restriction	Description
Change Location	The user can change move an object from one folder to another. All users having at least Browse permission on an object are granted Change Location permission by default for that object.
Change Ownership	The user can change the owner of the object.
Change State	The user can change the document lifecycle state of the object.
Change Permission	The user can change the basic permissions of the object.
Delete Object	The delete_object extended permission grants only the permission to delete an object. Unlike the base object-level Delete permission, the delete_object extended permission is not hierarchical. A user with delete_object extended permission has permission to delete an object, but not Browse, Read, Relate, Write, or Version permissions for the object.
Execute Procedure	The user can run the external procedure associated with the object. All users having at least Browse permission on an object are granted. Execute Procedure permission by default for that object.

The extended permissions are not hierarchical. An authorized user must assign each explicitly. Object-level permissions are defined as entries in ACL objects. Each SysObject (or SysObject subtype) object has an associated ACL. The entries in the ACL identify users and groups and define their object-level permissions to the object with which the ACL is associated. Superusers have Read permission by default on any object.

AccessRestriction and ExtendedRestriction Entries

Restriction entries restrict a user or group's access.

AccessRestriction Entries

An AccessRestriction entry removes the right to the base object-level permission level specified in the entry. The user or group members have access at the level up to the specified restriction. AccessRestriction entries are useful when an authorized user wants to give a group a particular base object-level permission, but restrict access for individual members or a subgroup of members. For example, suppose that Olivia is a member of the ProjTeam group and that an ACL has the following entries:

ACCESSOR_NAME: ProjTeam

PERMIT_TYPE: AccessPermit

PERMIT_LEVEL: delete

ACCESSOR_NAME: Olivia

PERMIT_TYPE: AccessRestriction

PERMIT_LEVEL: version

All members of the ProjTeam except Olivia have permission to delete objects governed by this ACL. Olivia's permission is restricted to browsing, reading, or annotating the objects even though she is a member of the ProjTeam. She cannot version the objects, or write or delete them.

ExtendedRestrictionEntries

An ExtendedRestriction entry restricts a user or the members of a specified group from exercising the specified extended object-level permission. For example, suppose that an ACL has the following entries and that HortenseJ is a member of the ProjTeam group:

ACCESSOR_NAME: ProjTeam_grp

PERMIT_TYPE: ExtendedPermit

PERMIT_LEVEL: change_owner,change_permit

ACCESSOR_NAME: HortenseJ

PERMIT_TYPE: ExtendedRestriction

PERMIT_LEVEL: change_permit

In this example, HortenseJ is restricted from the change_permit permission even though she is a member of a group whose members are granted this permission.

Storage in the ACL

In the ACL, both AccessRestriction entries and ExtendedRestriction entries for a particular user or group are stored in the same ACL entry, with the permit_type set to AccessRestriction. However, when an authorized user grants or revokes an AccessRestriction or ExtendedRestriction, an authorized user must specify whether AccessRestriction or ExtendedRestriction is being granted or revoked.

RequiredGroup Entries

A RequiredGroup entry requires a user requesting access to an object governed by the ACL to be a member of the group. For example, suppose an ACL has the following entries:

ACCESSOR_NAME: GaryG

PERMIT_TYPE: AccessPermit

PERMIT:Delete

ACCESSOR_NAME:ProjTeam

PERMIT_TYPE:RequiredGroup

PERMIT:NULL

ACCESSOR_NAME:Engr

PERMIT_TYPE:RequirdGroup

PERMIT:NULL

When GaryG attempts to access a document governed by this ACL, Content Server checks to determine whether he is a member of both the ProjTeam and Engr groups before allowing access. GaryG must belong to both groups. If he is not a member of both groups, the server does not allow him to access the document. The only exception to this is a superuser. A superuser is not required to be a member of any required group to access a document.

RequiredGroupSet Entries

A RequiredGroupSet entry requires a user requesting access to an object governed by the ACL to be a member of at least one group in the set. For example, suppose an ACL has the following entries:

ACCESSOR_NAME: HollyH

PERMIT_TYPE: AccessPermit

PERMIT:Delete

ACCESSOR_NAME:ProjTeam

PERMIT_TYPE:RequiredGroupSet

PERMIT:NULL

ACCESSOR_NAME:Engr

PERMIT_TYPE:RequirdGroupSet

PERMIT:NULL

When HollyH tries to access an object governed by this ACL, Content Server determines whether she is a member of either the ProjTeam or Engr group. She must be a member of one of these groups to be given access to the object. The only exceptions to this are superusers. A superuser is not required to be a member of any required group set to access a document. Each RequiredGroupSet entry identifies one group in the set. Consequently, an ACL that enforces a required group set typically has multiple RequiredGroupSet entries.

Table Permits

The table permits control access to the RDBMS tables represented by registered tables in the repository. To access an RDBMS table, a user must have:

- At least Browse access for the dm_registered object representing the RDBMS table
- The appropriate table permit for the operation that a user wants to perform

Superusers can access all RDBMS tables in the database using a SELECT statement regardless of whether the table is registered or not.

Table 6-8 Table Permits

Permit	Description
None	No access is permitted.
Select	The user can retrieve data from the table.
Update	The user can update existing data in the table.
Insert	The user can insert new data into the table.
Delete	The user can delete rows from the table.

The permits are not hierarchical. For example, assigning the permit to insert does not confer the permit to update. To assign more than one permit, add together the integers representing the permits wanted to assign and set the appropriate attribute to the total.

MUA-2 User attribute definition (FIA_ATD.1)

The TSF maintains the following user attributes:

- User identity,
- User State (active/inactive),
- Default Permission Set (A permission set to use to assign the default permissions to objects created by a user).
- Groups

- User Privileges (See Table 6-4),
- Extended User Privileges (See Table 6-5),
- Roles (Superuser, Sysadmin, User with Create Group, User with Create Cabinet, User with Create Type, and User),
- Turn off authentication failure checking.

MUA-3 User-subject binding (FIA_USB.1)

Content Server associates the appropriate user security attributes with subjects acting on behalf of that user.

MUA-4 Non-bypassability (FPT_RVM_EXP.1-1)

The TSF when invoked by the underlying host OS ensures that TOE Security Policy enforcement functions are invoked and succeed before each function within the TOE's Scope of Control is allowed to proceed. All management user operations are conducted in the context of an associated management session. This management session is allocated only after successful identification and authentication. User operations are checked for conformance to the granted level of access, and rejected if not conformant. The management session is destroyed when the corresponding user logs out of that session. Authorized users can only view the audit log(s), security attributes, and TSF data through a special administrative interface, and only after successfully identifying and authenticating themselves. Detailed system event audit records are kept which monitor events that occur in a repository. The audit logs are digitally signed to prevent and detect the modification of the audit records.

MUA-5 TSF domain separation (FPT_SEP_EXP.1-1)

The TSF when invoked by the underlying host OS maintains a security domain that protects it from interference and tampering by untrusted subjects in the TOE's Scope of Control. EMC Documentum Content Server is a passive device in that it indirectly connects to networks via other devices' e.g. network interface.

EMC Documentum's protected domain includes the EMC Documentum Content Server software and all of its software components.

In addition to the EMC Documentum Content Server-specific software, other software files such as configuration files are also stored on disk. EMC Documentum Content Server relies partially on the Operating System to provide file access permissions and identification and authentication of users at the OS level. In addition, EMC Documentum Content Server relies on the OS for file process separation. These files can be modified by an authorized user accessing them through the EMC Documentum Administrator interface. The Content Server User Access Control SFP is providing protection to accessing these files. The underlying assumption regarding the operation of EMC Documentum is that it is maintained in a physically secure environment.

6.1.4 Security Management Function

SM-1 Management of Security Functions Behavior (FMT_MOF.1)

The TSF shall restrict the ability to determine the behavior of, disable, enable, and modify the behavior of the functions related to the selection of which events are to be audited (see FAU_SEL.1.1) and audit (see FAU_GEN.1.1) to a User with Config Audit Privileges.

SM-2 Management of security attributes (FMT_MSA.1)

The Administrator can query, modify, create, and set and delete security attributes as specified in Table 5-2 in Section 5.2.

SM-3 Default Values of Security Attributes (FMT_MSA.3)

Content Server comes to the consumer with a number of security attributes enabled or disabled. The Superuser, Sysadmin, and User with Create Group Privileges are authorized to change the security attributes. Table 6-9 specifies the default security attributes and the default values.

Table 6-9 Security Attributes with Default Values

Security Attribute	Default Values
User Privileges	None (the lowest privilege level)
Extended User Privileges	A user has no extended user privileges by default.
Roles	SuperUser, Sysadmin, User **(These are "pre-defined" roles that have no default values assigned to them)**
Groups	Group name: docu (Users are assigned to the "docu" group by default when they are added to the repository. That means "if they are not explicitly assigned to another group by the person who creates them in the repository". The admin guide lists the users who are assigned to docu out of the box, i.e. when the docbase is configured. For example; the dm_autorender_win32/mac users are for the use of the AutoRenderPro client product to use when connecting the repository. Similarly, the dm_mediaserver user account is used by the EMC Documentum Transformation Services server to use when connecting to repository.) Members: repository_owner -> whoever is the owner of the repository installation_owner ---> whoever is the owner of the CS installation dm_autorender_win32 dm_autorender_mac dm_mediaserver Group Name: admingroup **(The admingroup group is created when the docbase is configured, but it is not used as default group for any user. i.e. it is never the default assigned value for the default_group attr in a user object)** Members: repository_owner -> whoever is the owner of the repository installation_owner ---> whoever is the owner of the CS installation
Base Object-level permissions and Restrictions	Base object-level permissions are controlled by ACL, so there are no defaults. A user has the permission, if any, assigned to him or her by the ACL associated with an object.
Extended Object-level permission and Restrictions	If user has at least Browse base permission level then the user also has Execute Procedure and Change Location permission. Otherwise, there are no default extended permissions.
User identity	Specifically this is the user_name security attribute and there is not a default value for this attribute.
User State (Active/Inactive)	Users are active by default when created in a repository.
Default Permission Set	A user's default ACL is chosen by the person creating the user in the repository. If said person fails to specify a default permission set, then Content Server sets the permission. Which ACL is assigned is dependent on the repository's configuration.
Turn off authentication failure	Authentication failure checking is off by default in a repository. It must be manually activated by setting a configuration attribute (max_auth_attempt) in the repository

Security Attribute	Default Values
checking	config object.

SM-4 Management of TSF Data (FMT_MTD.1)

The allowed operations on TSF Data and the authorized roles required to execute them are listed in Table 5-3 in Section 5.2.

SM-5 Specification of Management Functions (FMT_SMF.1)

The Content Server is capable of performing the following security management functions:

- determine the behavior of, disable, enable, and modify the behavior of the functions related to the selection of which events are to be audited (see FAU_SEL.1.1) and audit (see FAU_GEN.1.1) (see FMT_MOF.1),
- query, modify, and delete the security attributes as specified in Table 5-2 (see FMT_MSA.1),
- query, modify, delete, and create as specified in Table 5-3 and the TSF Data as specified in Table 5-3 (See FMT_MTD.1).

SM-6 Security Roles (FMT_SMR.1)

The TOE maintains seven predefined trusted user roles:

- Superuser,
- Sysadmin,
- User with Create Group,
- User with Create Cabinet,
- User with Create Type, and
- User

6.1.5 SOF Claims

There are no specific SOF claims pertaining to a specific IT Security Function(s) since FIA_SOS.1 is not included as a TOE SFR. A general SOF claim for all of these IT security functions is SOF-Basic.

6.2 Assurance Measures

The EMC Documentum Content Server satisfies the assurance requirements for Evaluation Assurance Level EAL2

The following items are provided as evaluation evidence to satisfy the EAL2 assurance requirements:

Table 6-10 Assurance Measures

Item	Component	Evidence Requirements	How Satisfied
1	ACM_CAP.2	CM	Document_ACM_v0.2.doc

Item	Component	Evidence Requirements	How Satisfied
		Documentation • CM Proof • Configuration Item List	EMC Documentum Content Server V 5.3 and EMC Documentum Administrator V5.3 Configuration Management Capabilities, Version 0.3 June 25, 2005
			StarTeam_End_User_Training_Guide_SHORT_VERSION Version 1.0, October 1 2005
			StarTeam**_FAQ** Version 1.0, October 1 2005
			StarTeam_Getting_Started Version 1.0, October 1 2005
2	ADO_DEL.1	Delivery Procedures	EMC Documentum Content Server V 5.3 and EMC Documentum Administrator V5.3 Secure Delivery Document, Version 0.3 June 24, 2005
3	ADO_IGS.1	Installation, generation, and start-up procedures	Content Server Installation Guide V5.3 WDK_53_applications_installation.pdf, Web Development Kit and Applications Installation Guide, Version 5.3, March 2005
4	ADV_FSP.1	Functional Specification	EMC Documentum Content Server V 5.3 and EMC Documentum Administrator V5.3 Functional Specification, Version 1.0 Final, August 23, 2005
5	ADV_HLD.1	High-Level Design	EMC Documentum Content Server V 5.3 and EMC Documentum Administrator V5.3 Descriptive High-Level Design Version 0.3 August 01, 2005
6	ADV_RCR.1	Representation Correspondence	EMC Documentum Content Server V 5.3 and EMC Documentum Administrator V5.3 Vulnerability Analysis, Version 1.0 Final, August 23, 2005
7	AGD_ADM.1	Administrator Guidance	
			Content Server Administrator's Guide V5.3, Version 5.3 March 2005
			Content Server API Reference Manual, Version 5.3 March 2005
			Distributed Configuration Guide Version 5.3, March 2005

Item	Component	Evidence Requirements	How Satisfied
			Content Server DQL Reference Manual, Version 5.3 March 2005
			Content Server Fundamentals Version 5.3, March 2005
			EMC Documentum Content Server Combined Index, Version 5.3 March 20005
			Content Server Installation Guide Version 5.3, April 2005
			Content Server Object Reference Manual, Version 5.3, March 2005
			EMC Documentum Content Server Release Notes, Version 5.3 May 2005
			EMC Documentum Administrator Release Notes, Version 5.3 July, 2005
			EMC Documentum Administrator User Guide, Version 5.3, March 2005
			EMC Documentum Content Server V 5.3 and EMC Documentum Administrator V5.3 Common Criteria Supplement Guide, Version 0.1 June 06, 2005

Item	Component	Evidence Requirements	How Satisfied
8	AGD_USR.1	User Guidance	EMC Documentum Administrator User Guide, Version 5.3, March 2005
			Content Server Installation Guide Version 5.3, April 2005
			Content Server Administrator's Guide V5.3, Version 5.3 March 2005
			Content Server Fundamentals Version 5.3, March 2005
			StarTeam_End_User_Training_Guide_SHORT_VERSION Version 1.0, October 1 2005
			StarTeam**_FAQ** Version 1.0, October 1 2005
			StarTeam_Getting_Started Version 1.0, October 1 2005
9	ATE_COV.1	Test Coverage Analysis	EMC Documentum Content Server V 5.3 and EMC Documentum Administrator V5.3 Test Coverage Analysis V2.1 July, 20 2005
10	ATE_FUN.1	Test Documentation	DA Common Criteria Test Evidence.Doc
11	ATE_IND.2	TOE for Testing	TOE for Testing
12	AVA_SOF.1	SOF Analysis	EMC Documentum Content Server V 5.3 and EMC Documentum Administrator V5.3 Vulnerability Analysis, Version 1.0 Final, August 23, 2005
13	AVA_VLA.1	Vulnerability Analysis	EMC Documentum Content Server V 5.3 and EMC Documentum Administrator V5.3 Vulnerability Analysis, Version 1.0 Final, August 23, 2005

7 PP Claims

The EMC Documentum Content Server Security Target was not written to address any existing Protection Profile.

8 Rationale

8.1 Security Objectives Rationale

8.1.1 Threats to Security

Table 8-1 shows that all the identified threats to security are countered by Security Objectives for the TOE.

Table 8-1 All Threats to Security Countered

Item	Threat Name	Security Objective
1	T.Abuse	O.Access O.Attributes O.Audit OE.IDAuth OE.Time
2	T.Access	O.Access O.Attributes O.Audit OE.AuditProtect OE.IDAuth OE.Time
3	T.Bypass	O.NonBypass OE.NonBypass
4	T.Mismanage	O.Admin O.Roles
5	T.Privilege	O.Access O.Attributes O.PartialDomainSep OE.PartialDomainSep OE.IDAuth
6	T.Tamper	O.PartialDomainSep OE.PartialDomainSep
7	T.Undetect	O.Audit OE.Time

T.Abuse: An undetected compromise of the TOE may occur as a result of an authorized user of the TOE (intentionally or otherwise) performing actions the individual is authorized to perform. T.Abuse is countered by:

- O.Access: The TOE will allow authorized TOE users to access only authorized TOE functions and data. This is provided by access controls that limit the actions an individual is authorized to perform.

- O.Attributes: The TOE will be able to maintain user security attributes. This objective counters this threat by requiring the TOE to store and maintain attributes. These attributes associate users with user accounts and privileges that the EMC Documentum eBusiness Access Control Policy is based on.
- O.Audit: The TOE will record audit records for data accesses and use of the system functions. This objective counters this threat by requiring the TOE to audit attempts for data accesses and use of TOE functions.
- OE.IDAuth: The IT environment will be able to identify and authenticate users prior to allowing access to authorized TOE functions and data. This objective provides for authentication of users prior to any TOE data access.
- OE.Time: The IT environment will provide reliable time stamps. This objective provides for a reliable way to correlate audit records to reconstruct a potential compromise.

T.Access: An authorized user of the TOE may access information or resources without having permission from the person who owns, or is responsible for, the information or resource. T.Access is countered by:

- O.Access: The TOE will allow authorized TOE users to access only authorized TOE functions and data. This is provided by access controls that limit the actions an individual is authorized to perform.
- O.Attributes: The TOE will be able to maintain user security attributes. This objective counters this threat by requiring the TOE to store and maintain attributes. These attributes associate users with user accounts and privileges that the EMC Documentum eBusiness Access Control Policy is based on.
- O.Audit: The TOE will record audit records for data accesses and use of the system functions. This objective counters this threat by requiring the TOE to audit attempts for data accesses and use of TOE functions.
- OE.AuditProtect: The IT environment will ensure the protection of the audit storage. This objective counters this threat by requiring the IT Environment to provide protection of the audit storage.
- OE.IDAuth: The IT environment will be able to identify and authenticate users prior to allowing access to authorized TOE functions and data. This objective provides for authentication of users prior to any TOE data access.
- OE.Time: The IT environment will provide reliable time stamps. This objective provides for a reliable way to correlate audit records to reconstruct a potential compromise.

T.Bypass: An attacker may attempt to bypass TSF security functions to gain unauthorized access to TSF. T.Bypass is countered by:

- O.NonBypass: The TOE will ensure that the security enforcing functions are invoked and succeed before allowing a TOE function to proceed. This objective counters this threat by ensuring the TOE's protection mechanisms cannot be bypassed, which requires that TSF security functions not be bypassable.
- OE.NonBypass: The IT environment will ensure the security enforcing functions are invoked and succeed before allowing a TOE function to proceed. This objective counters this threat by the IT Environment (underlying Operating System) ensuring the TOE's protection mechanisms cannot be bypassed, which requires that TSF security functions not be bypassable.

T.Mismanage: Administrative errors may allow attackers to gain unauthorized access to resources protected by the TOE. T.Mismanage is countered by:

- O.Admin: The TOE will provide the functionality to enable an authorized user to effectively manage the TOE and its security functions. Administrative tools make it easier for administrators to correctly manage the TOE.

- O.Roles: The TOE will support multiple administrative roles. Multiple administrative roles can be used to enforce separation of duty, so that one authorized administrator can catch errors made by another authorized administrator.

T.Privilege: An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data. T.Privilege is countered by:

- O.Access: The TOE will allow authorized TOE users to access only authorized TOE functions and data. This objective builds upon the OE.IDAuth objective by only permitting authorized users to access TOE functions.
- O.Attributes: The TOE will be able to maintain user security attributes. This objective counters this threat by requiring the TOE to store and maintain attributes. These attributes associate users with user accounts and privileges that the EMC Documentum eBusiness Access Control Policy is based on.
- O.PartialDomainSep: The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering or unauthorized disclosure, through its own interfaces. This objective addresses this threat by providing TOE self-protection and separation between users. The TOE will provide separation between code executing on behalf of different users.
- OE.PartialDomainSep: The IT environment will protect TOE programs and data from unauthorized modification. This objective addresses this threat by protecting the TOE and its data.
- OE.IDAuth: The IT environment will be able to identify and authenticate users prior to allowing access to authorized TOE functions and data. This objective provides for authentication of users prior to any TOE function access.

T.Tamper: An attacker may attempt to modify TSF programs and data. T.Tamper is countered by:

- O.PartialDomainSep: The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering or unauthorized disclosure, through its own interfaces. This objective addresses this threat by providing TOE self-protection and separation between users. The TOE will provide separation between code executing on behalf of different users.
- OE.PartialDomainSep: The IT environment must protect TOE programs and data from unauthorized modification. This objective addresses this threat by protecting the TOE and its data.

T.Undetect: Attempts by an attacker to violate the security policy may go undetected. If the attacker is successful, TSF data may be lost or altered. T.Undetect is countered by:

- O.Audit: The TOE will record audit records for data accesses and use of the system functions. This objective records attempts to violate the security policy.

OE.Time: The IT environment will provide reliable time stamps. This objective provides for a reliable way to correlate audit records to reconstruct a potential compromise.

Table 8-2 Reverse Mapping of TOE Security Objectives to Threats

Note: This table is provided to show completeness by demonstrating all security objectives for the TOE map to at least one threat.

Item	Objective	Threat
1	O.Access	T.Abuse T.Access T.Privilege
2	O.Admin	T.Mismanage
3	O.Attributes	T.Abuse

		T.Access T.Privilege
4	O.Audit	T.Abuse T.Access T.Undetect
5	O.NonBypass	T.Bypass
6	O.PartialDomainSep	T.Tamper T.Privilege
7	O.Roles	T.Mismanage

8.1.2 Assumptions

Table 8-3 shows that all of the secure usage assumptions are addressed by either security objectives for the IT environment or Non-IT security objectives. Rationale for each assumption is provided below the table.

Table 8-3 All Assumptions Addressed

No	Name	Objective
1	A.Admin	ON.Install ON.Operations
3	A.Database	ON.Install
4	A.NoUntrusted	ON.NoUntrusted
5	A.OS	ON.Install
6	A.Physical	ON.Physical
7	A.ProtectComm	ON.ProtectComm
8	A.Time	OE.Time

A.Admin: The authorized administrator is trusted to correctly configure and operate the TOE according to the instructions provided by the TOE documentation. A.Admin is covered by:

- ON.Install: Those responsible for the TOE must ensure that the TOE is delivered and installed in a manner that maintains IT security. Installing the TOE in a manner that maintains IT security includes correctly configuring the TOE. This objective provides for secure installation and configuration of the TOE.
- ON.Operations: The TOE will be managed and operated in a secure manner as outlined in the supplied guidance. The procedures will provide guidance to the authorized administrator on how to securely operate the TOE. This objective provides for operation procedures to be in place.

A.Database The IT environment provides a database to store TSF data. A.Database is covered by:

- ON.Install: Those responsible for the TOE must ensure that the TOE is delivered and installed in a manner that maintains IT security. Installing the TOE in a manner that maintains IT security includes installing the EMC Documentum Content Server according to the product's installation requirements. This includes installing the Oracle database according to the Guidance documentation. This objective provides for secure installation of the TOE.

A.NoUntrusted: There are no untrusted users and no untrusted software on the EMC Documentum Content Server host. A.NoUntrusted is covered by:

- ON.NoUntrusted: The authorized administrator must ensure that there are no untrusted users and no untrusted software on the EMC Documentum Content Server host. This objective corresponds directly to the assumption.

A.ProtectComm: Those responsible for the TOE will ensure the communications between the EMC Documentum Administrator and EMC Documentum Content Server host are secure.

- ON.ProtectComm: Those responsible for the TOE will protect communications between the EMC Documentum Administrator and EMC Documentum Content Server host. This objective provides for the secure communications between the EMC Documentum Administrator and EMC Documentum Content Server host.

A.OS: The OS provides file protection and user authentication. A.OS is covered by:

- ON.Install: Those responsible for the TOE must ensure that the TOE is delivered and installed in a manner that maintains IT security. Installing the TOE in a manner that maintains IT security includes installing the EMC Documentum Content Server on recommended Operating Systems according to the product's installation requirements and Guidance documentation. This objective provides for secure installation of the TOE.

A.Physical: The TOE components critical to the security policy enforcement will be protected from unauthorized physical modification by being located within controlled access facilities and behind a Firewall. A.Physical is covered by:

- ON.Physical: Those responsible for the TOE must ensure that those parts of the TOE critical to the security policy are protected from any physical attack. This objective provides for the physical protection of the TOE components.

A.Time: The underlying operating system provides reliable time stamps. A.Time is covered by:

- OE.Time: The IT environment will provide reliable time stamps. This objective provides for reliable time stamps.

Table 8-4 Reverse Mapping of Security Objectives for the Environment to Assumptions/Threats

Note: This table is provided to show completeness by demonstrating all security objectives for the environment map to at least one assumption or threat.

No.	Objective Name	Threat/Policy/Assumption
9E	OE.AuditProtect	T.Access
10E	OE.IDAuth	T.Abuse T.Access T.Privilege
11E	OE.NonBypass	T.Bypass
12E	OE.PartialDomainSep	T.Privilege T.Tamper
13E	OE.Time	A.Time T.Abuse T.Access T.Undetect

8.2 Security Requirements Rationale

8.2.1 Functional Requirements

Table 8-5 shows that all of the security objectives of the TOE are satisfied.

Table 8-5 All Objectives Met by Functional Components

Item	Objective	Security Functional Requirement
1	O.Access	FAU_SAR.2 Restricted audit review FDP_ACC.2 Complete access control FDP_ACF.1 Security attribute based access control FIA_USB.1 User subject binding FMT_MOF.1 Management of security functions behavior FMT_MTD.1 Management of TSF data
2	O.Admin	FAU_SAR.1 Audit review FAU_SAR.3 Selectable audit review FAU_SEL.1 Selective audit FMT_MOF.1 Management of security functions behaviour FMT_MSA.1 Management of security attributes FMT_MSA.3 Static attribute initialisation FMT_MTD.1 Management of TSF data FMT_SMF.1 Specification of management functions
3	O.Attributes	FIA_ATD.1 User attribute definition

Item	Objective	Security Functional Requirement
4	O.Audit	FAU_GEN.1 Audit data generation FAU_GEN.2 User identity association FAU_SEL.1 Selective audit FAU_STG_EXP.1-1 Protected audit trail storage
5	O.NonBypass	FPT_RVM_EXP.1-1 Non-bypassability of the TSP
6	O.PartialDomainSep	FPT_SEP_EXP.1-1 TSF domain separation
7	O.Roles	FMT_SMR.1 Security roles

O.Access: The TOE will allow authorized TOE users to access only authorized TOE functions and data. O.Access is addressed by:

- FAU_SAR.2 Restricted audit review, which requires that access to audit data be restricted to authorized users.
- FDP_ACC.2 Complete access control, which requires that the TSF enforce access controls on all operations between any subject in the TSC and any object within the TSC.
- FDP_ACF.1 Security attribute based access control, which requires the TSF enforce access controls based on specified security attributes. In addition, the TSF can explicitly authorize and deny access to specified subjects.
- FIA_USB.1 User subject binding, which requires that the TSF associates all user security attributes with subjects acting on behalf of the user.
- FMT_MOF.1 Management of security functions behavior, which restricts the ability to disable, enable, and modify functions to authorized users.
- FMT_MTD.1 Management of TSF data, which specifies the management of TSF Data according to assigned roles.

O.Admin: The TOE will provide the functionality to enable an authorized user to effectively manage the TOE and its security functions. O.Admin is addressed by:

- FAU_SAR.1 Audit review, which requires that users with Superuser or View Audit privileges be able to read all audit information from the audit records.
- FAU_SAR.3 Selectable audit review, which requires that the TSF will provide the ability to search audit data.
- FAU_SEL.1 Selective audit, which requires the TOE to provide authorized users with the ability to include or exclude auditable events from the set of audited events.
- FMT_MOF.1 Management of security functions behaviour, which requires that the auditor be able to manage the behavior of the audit tools
- FMT_MSA.1 Management of security attributes, which requires only authorized users can query, modify, and delete specified security attributes.
- FMT_MSA.3 Static attribute initialization, which requires the TSF to enforce access control to restrict access to specified default values of security attributes.
- FMT_MTD.1 Management of TSF data, which specifies the management of TSF Data according to assigned roles.

- FMT_SMF.1 Specification of management functions, which requires the TSF be capable of performing the specified security management functions.

O.Audit: The TOE will record audit records for data accesses and use of the system functions. O.Audit is addressed by:

- FAU_GEN.1 Audit data generation, which requires the ability to audit specified events.
- FAU_GEN.2 User identity association, which requires the ability to associate an auditable event with a specific user.
- FAU_SEL.1 Selective audit, which requires the TOE to provide authorized users with the ability to include or exclude auditable events from the set of audited events.
- FAU_STG_EXP.1-1 Protected audit trail storage, which requires the TSF to protect audit records from unauthorized deletion and prevent unauthorized modifications.

O.PartialDomainSep: The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering or unauthorized disclosure, through its own interfaces. O.PartialDomainSep is addressed by:

- FPT_SEP_EXP.1-1 TSF domain separation, which requires that the TSF maintain a security domain for its own execution that protects it from interference and tampering by untrusted users. The TSF must enforce separation between security domains of subjects in the TSC.

O.Attributes: The TOE must be able to maintain user security attributes. O.Attributes is addressed by:

- FIA_ATD.1 User attribute definition, which requires that the TSF maintain security attributes of users.

O.NonBypass: The TOE will ensure that the security enforcing functions are invoked and succeed before allowing a TOE function to proceed. O.NonBypass is addressed by:

- FPT_RVM_EXP.1-1 Non-bypassability of the TSP, which requires that TSP enforcement functions are invoked and succeed before a security-relevant function is allowed to proceed.

O.Roles: The TOE will support multiple administrative roles. O.Roles is addressed by:

- FMT_SMR.1 Security roles, which requires that the TSF maintain multiple administrative roles.

Table 8-6 Reverse Mapping of TOE Functional Requirements to IT Security Objectives

Note: This table has been included as a consistency check to show that the TOE security functional requirements for the IT environment map to the TOE security objectives.

No.	Requirement	Component Name	Objective
1	FAU_GEN.1	Audit data generation	O.Audit
2	FAU_GEN.2	User identity association	O.Audit
3	FAU_SAR.1	Audit review	O.Admin
4	FAU_SAR.2	Restricted audit review	O.Access
5	FAU_SAR.3	Selectable audit review	O.Admin
6	FAU_SEL.1	Selective audit	O.Admin O.Audit
7	FAU_STG_EXP.1-1	Protected audit trail storage	O.Audit

No.	Requirement	Component Name	Objective
8	FDP_ACC.2	Complete access control	O.Access
9	FDP_ACF.1	Security attribute based access control	O.Access
10	FIA_ATD.1	User attribute definition	O.Attributes
11	FIA_USB.1	User-subject binding	O.Access
12	FMT_MOF.1	Management of security functions behavior	O.Access O.Admin
13	FMT_MSA.1	Management of security attributes	O.Admin
14	FMT_MSA.3	Static attribute initialisation	O.Admin
15	FMT_MTD.1	Management of TSF data	O.Access O.Admin
16	FMT_SMF.1	Specification of management functions	O.Admin
17	FMT_SMR.1	Security roles	O.Roles
18	FPT_RVM_EXP.1	Non-bypassability of the TSP	O.NonBypass
19	FPT_SEP_EXP.1-1	Domain separation	O.PartialDomainSep

8.2.2 Dependencies

Table 8-7 shows the dependencies between the functional requirements. All dependencies are satisfied. Dependencies that are satisfied by a hierarchical component are denoted by an (H) following the dependency reference.

Table 8-7 TOE Dependencies Satisfied

No.	Component	Component Name	Dependencies	Reference
1	FAU_GEN.1	Audit data generation	FPT_STM.1	25
2	FAU_GEN.2	User identity association	FAU_GEN.1	1
3	FAU_SAR.1	Audit Review	FAU_GEN.1	1
4	FAU_SAR.2	Restricted audit review	FAU_SAR.1	3
5	FAU_SAR.3	Selectable audit review	FAU_SAR.1	3
6	FAU_SEL.1	Selective audit	FAU_GEN.1	1
			FMT_MTD.1	15
7	FAU_STG_EXP.1-1	Protected audit trail storage	FAU_GEN.1	1
8	FDP_ACC.2	Complete access control	FDP_ACF.1	9
9	FDP_ACF.1	Security attribute based access control	FDP_ACC.1	8 (H)
			FMT_MSA.3	14
10	FIA_ATD.1	User attribute definition	None	None
11	FIA_USB.1	User subject binding	FIA_ATD.1	10
12	FMT_MOF.1	Management of security functions behavior	FMT_SMR.1	17
			FMT_SMF.1	16
13	FMT_MSA.1*	Management of security attributes	FDP_ACC.1	8 (H)

No.	Component	Component Name	Dependencies	Reference
			FMT_SMR.1	17
			FMT_SMF.1	16
14	FMT_MSA.3	Static attribute initialization	FMT_MSA.1	13
			FMT_SMR.1	17
15	FMT_MTD.1	Management of TSF data	FMT_SMR.1	17
			FMT_SMF.1	16
16	FMT_SMF.1	Specification of management functions	None	None
17	FMT_SMR.1	Security roles	FIA_UID.1	22 (H)
18	FPT_RVM_EXP.1	Non-bypassability of the TSP	None	None
19	FPT_SEP_EXP.1-1	TSF domain separation	None	None

Table 8-8 IT Environment Dependencies Satisfied

Item	Component	Component Name	Dependencies	Reference
20	FAU_STG_EXP.1-2	Protected audit trail storage	FAU_GEN.1	1
21	FIA_UAU.2	User authentication before any action	FIA_UID.1	22 (H)
22	FIA_UID.2	User identification before any action	None	None
23	FPT_RVM_EXP.1-1	Non-bypassability of the TSP	None	None
24	FPT_SEP_EXP.1-2	TSF domain separation	None	None
25	FPT_STM.1	Reliable time stamps	None	None

8.2.3 Strength of Function

A strength of function level of SOF-Basic counters an attack level of low. The environment is one where the potential attacker is unsophisticated, with access to only standard equipment and public information about the product.

8.2.4 Assurance Requirements

Evaluation Assurance Level EAL2 was chosen to provide a basic level of assurance due to the low level threat of malicious attacks.

8.2.5 Rationale that IT Security Requirements are Internally Consistent

The IT Security Requirements are internally consistent. There are no requirements that conflict with one another. When different IT security requirements apply to the same event, operation, or data there is no conflict between the security requirements. The requirements mutually support each other to apply to the event, operation, or data.

For auditing, each of the SFRs build on the others. Audit records are generated for many events where other requirements are coming to bear, such as login, policy check failures, and management functions. For example, FAU_GEN.1 details the auditable events generated by the TSF. FAU_GEN.2 provides for the TSF to associate each auditable event with the identity of the user that caused the event. FAU_SAR.1 states that the specified authorized users are able to read specified audit information. FAU_SAR.2 builds on FAU_SAR.1 by stating the TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access. FAU_SAR.3 gives the authorized administrator the ability to perform searches of the audit event data. FAU_SEL.1 allows the authorized administrator to include or exclude auditable events from the set of audited events. FAU_STG_EXP.1-1 provides for partial protection of the storage of the audit data.

Together FDP_ACC.2 and FDP_ACF.1 provide User Data Protection. FDP_ACC.2 defines the Content Server User Access Control SFP. FDP_ACF.1 specifies that the TSF enforce access based upon security attributes and named groups of attributes. The subjects with roles of the following listed in Table 5-2 (FDP_ACC.2) are also defined in FMT_SMR.1.

FIA_ATD.1 specifies the security attributes belonging to individual users.

The management requirements (FMT_) are related to many of the mechanisms involved with other requirements. FMT_MOF.1 provides for the management of the audit functions (FAU_GEN.1 and FAU_SEL.1). FMT_MSA.1 enforces the Content Server User Access Control SFP (FDP_ACC.2). FMT_MSA.3 enforces the Content Server User Access Control SFP to provide restrictive default values for security attributes. FMT_MTD.1 specifies the management of TSF Data according to assigned roles. FMT_SMF.1 specifies the security management functions of the TSF. In many cases, the other mechanisms will enforce the settings made through management functions. Installation mechanisms (see ADO_IGS.1) rely on management functions. The administrator guidance (see AGD_ADM) documents the management functions.

FPT_RVM_EXP.1 makes certain the Content Server User Access Control SFP (FDP_ACC.2) is invoked and succeeds before any other functions within the TOE's Scope of Control are allowed to proceed. FPT_SEP_EXP.1-1 relies on FDP_ACC.2 to provide protection against unauthorised subjects from gaining access to the TOE's administrator interface.

8.2.6 Explicitly Stated Requirements Rationale

FPT_RVM_EXP.1, FPT_SEP_EXP.1, and FAU_STG_EXP.1 had to be explicitly stated because they all provide partial TOE self-protection while relying on the OS and Hardware platforms to provide the full protection. According to CCIMB RI#19, which states the following: "Where necessary to cover different aspects of the same requirement (e.g. identification of more than one type of user), repetitive use (i.e. applying the operation of iteration) of the same Part 2 components to cover each aspect is possible. The statement of TOE security requirements shall define the functional and assurance security requirements that the TOE and the supporting evidence for its evaluation need to satisfy in order to meet the security objectives for the TOE. Since the iterations of FPT_RVM_EXP.1, FPT_SEP_EXP.1, and FAU_STG_EXP.1 span both the TOE requirements and IT Environment, they must be explicitly stated.

8.2.7 Requirements for the IT Environment

Table 8-9 shows that all of the security objectives for the IT environment are satisfied.

Table 8-9 All Objectives for the IT Environment Met by Requirements

Item	Objective	Requirement for the IT Environment	Component Title
9E	OE.AuditProtect	FAU_STG_EXP.1-2	Protected audit trail storage
10E	OE.IDAuth	FIA_UAU.2	User authentication before any action
		FIA_UID.2	User identification before any action
11E	OE.NonBypass	FPT_RVM_EXP.1-2	Non-bypassability of the TSP
12E	OE.PartialDomainSep	FPT_SEP_EXP.1-2	TSF domain separation
13E	OE.Time	FPT_STM.1	Reliable time stamps

OE.AuditProtect: The IT environment will ensure the protection of the audit storage. OE.AuditProtect is addressed by:

- FAU_STG_EXP.1-2 Protected audit trail storage, which requires the IT environment to protect the stored audit records in the audit trail from unauthorized deletion and can prevent unauthorized modifications to the audit records in the audit trail. The TOE relies on the underlying OS, DBMS, and hardware to protect the audit trail storage.

OE.IDAuth: The IT environment will be able to identify and authenticate users prior to allowing access to authorized TOE functions and data. OE.IDAuth is addressed by:

- FIA_UAU.2 User authentication before any action, which requires the IT environment to authenticate each user successfully before allowing access to the TOE.
- FIA_UID.2 User identification before any action, which requires the IT environment to successfully identify each user before allowing access to the TOE.

OE.NonBypass: The IT environment will ensure the security enforcing functions are invoked and succeed before allowing a TOE function to proceed. OE.NonBypass is addressed by:

- FPT_RVM_EXP.1-2 Non-bypassability of the TSP, which requires that the IT Environment ensures the OS enforcement functions are invoked and succeed before a security-relevant function is allowed to proceed.

OE.PartialDomainSep: The IT environment will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure, through its own interfaces. OE.PartialDomainSep is addressed by:

- FPT_SEP_EXP.1-2 TSF domain separation, which requires the Operating System to maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects initiating actions through the Operating System's Interface. The IT environment must enforce separation between security domains of subjects in the Operating System's Scope of Control.

OE.Time: The IT environment will provide reliable time stamps. OE.Time is addressed by:

- FPT_STM.1 Reliable time stamps, which requires that time stamps be provided by the IT environment.

Table 8-10 Reverse Mapping of Environment SFRs to Environment Security Objectives

Note: This table has been provided for completeness to show that all security functional requirements map to at least on TOE Security Objective.

Item	Environment SFRs	Environment Security Objectives
20	FAU_STG_EXP.1-2	OE.AuditProtect
21	FIA_UAU.2	OE.IDAuth
22	FIA_UID.2	OE.IDAuth
23	FPT_RVM_EXP.1-2	OE.NonBypass
24	FPT_SEP_EXP.1-2	OE.PartialDomainSep
25	FPT_STM.1	OE.Time

8.3 TOE Summary Specification Rationale

8.3.1 IT Security Functions

Table 8-11 shows that the IT Security Functions in the TOE Summary Specification (TSS) address all of the TOE Security Functional Requirements.

Table 8-11 Mapping of Functional Requirements to TOE Summary Specification

No.	Security Functional Requirement	Security Functional Component	Requirement is met by:	
			Security Function Ref. No	Rationale
1	FAU_GEN.1	Audit data generation	SA-1	Specifies the types of events to be audited and the information to be recorded in an audit record. .
2	FAU_GEN.2	User identity association	SA-2	Each auditable event is associated with the identity of the user that caused the event.
3	FAU_SAR.1	Audit review	SA-3	Specifies who has the capability to read information from the audit records.
4	FAU_SAR.2	Restricted audit review	SA-4	Specifies that only specific users have read access to the audit records.
5	FAU_SAR.3	Selectable audit review	SA-5	Specifies EMC Documentum Content Server provides the ability to perform searches of the audit data based on various criteria.
6	FAU_SEL.1	Selective audit	SA-6	Specifies EMC Documentum Content Server is able to include or exclude auditable events from the set of audited events based on specific attributes.
7a	FAU_STG_EXP.1-1	Protected audit trail storage	SA-7	Specifies EMC Documentum Content Server is able to prevent unauthorized modifications to the audit records.
8	FDP_ACC.2	Complete access control	MUA-1	Specifies the Content Server User Access Control SFP.
9	FDP_ACF.1	Security attribute based access control	MUA-1	Specifies the subjects and objects controlled under the Content Server User Access Control SFP.
10	FIA_ATD.1	User attribute definition	MUA-2	Specifies the security attributes maintained for each user.
11	FIA_USB.1	User subject binding	MUA-3	Specifies that the user shall associate all user security attributes with subjects acting on behalf of that user.

No.	Security Functional Requirement	Security Functional Component	Requirement is met by:	
			Security Function Ref. No	Rationale
12	FMT_MOF.1	Management of security functions behavior	SM-1	Specifies that the EMC Documentum Content Server restricts the ability to determine the behavior of, disable, enable, and modify the behavior of the functions related to the selection of which events are to be audited (see FAU_SEL.1.1) and the audit function (see FAU_GEN.1.1) to a User with Config Audit Privileges.
13	FMT_MSA.1	Management of security attributes	SM-2	Specifies that the ability to query, modify, delete, or create the specified security attributes see Table 5-2 is restricted to the specified users see Table 5-2.
14	FMT_MSA.3	Static attribute initialisation	SM-3	Specifies that the EMC Documentum Content Server provides restrictive default values for security attributes and the Superuser, Sysadmin, and User with Create Group Privileges can specify alternative initial values.
15	FMT_MTD.1	Management of TSF data	SM-4	Specifies that the EMC Documentum Content Server restricts the ability to manage TSF data.
16	FMT_SMF.1	Specification of management functions	SM-5	Specifies the security management functions provided by the EMC Documentum Content Server.
17	FMT_SMR.1	Security roles	SM-6	Specifies the roles maintained.
18	FPT_RVM_EXP.1	Non-bypassability of the TSP	MUA-4	Specifies that the EMC Documentum Content Server ensures that the Content Server User Access Control SFP is invoked and succeeds before each function is allowed to proceed.
19	FPT_SEP_EXP.1-1	TSFDomain separation	MUA-5	Specifies that the EMC Documentum Content Server maintains a security domain for its own execution and enforces separation between the security domains of users. The Content Server User Access Control SFP is used to protect the TSF data from tampering.

8.3.2 Assurance Measures

The assurance measures rationale shows how all assurance requirements are satisfied. The rationale is provided in Table 8-12.

Table 8-12 Assurance Measures Rationale

Item	Component	Evidence Requirements	How Satisfied	Rationale
1	ACM_CAP.2	CM Documentation • CM Proof • Configuration Item List	EMC Documentum Content Server V 5.3 and EMC Documentum Administrator V5.3 Configuration Management Capabilities, Version 0.3 June 25, 2005 Document_ACM_v0.2.doc StarTeam_End_User_Training_Guide_SHORT_VERSION Version 1.0, October 1 2005 StarTeam**_FAQ** Version 1.0, October 1 2005 StarTeam_Getting_Started Version 1.0, October 1 2005	• CM Proof - Shows the CM system is being used. • Configuration Item List(s) - is comprised of a list of the source code files and version numbers - is comprised of a list of design documents with version numbers - is comprised of test documents with version numbers - user and administrator documentation with version numbers
2	ADO_DEL.1	Delivery Procedures	EMC Documentum Content Server V 5.3 and EMC Documentum Administrator V5.3 Secure Delivery Document, Version 0.3 June 24, 2005	Provides a description of all procedures that are necessary to maintain security when distributing Access Control software to the user's site. - Applicable across all phases of delivery from packaging, storage, distribution

Item	Component	Evidence Requirements	How Satisfied	Rationale
3	ADO_IGS.1	Installation, generation, and start-up procedures	Content Server Installation Guide V5.3 WDK_53_applications_installation.pdf, Web Development Kit and Applications Installation Guide, Version 5.3, March 2005	Provides detailed instructions on how to install EMC Documentum Content Server.
4	ADV_FSP.1	Functional Specification	EMC Documentum Content Server V 5.3 and EMC Documentum Administrator V5.3 Functional Specification, Version 1.0 Final, August 23, 2005	Provides rationale that TSF is fully represented. A bi-directional mapping of security functions to guidance documentation.
			Content Server Administrator's Guide V5.3	Describes the TSF interfaces and TOE functionality
			EMC Documentum Administrator User Guide V5.3	Describes the TSF interfaces and TOE functionality
			Content Server Fundamentals V5.3	Describes the TSF interfaces and TOE functionality
			Content Server API Reference Manual V5.3	
5	ADV_HLD.1	High-Level Design	EMC Documentum Content Server V 5.3 and EMC Documentum Administrator V5.3 Descriptive High-Level Design Version 0.3 August 01, 2005	Describes the TOE subsystems and their associated security functionality
6	ADV_RCR.1	Representation Correspondence	EMC Documentum Content Server V 5.3 and EMC Documentum Administrator V5.3 Vulnerability Analysis, Version 1.0 Final, August 23, 2005 Documentation will be provided that includes correspondence analysis between: 1. TSS and functional specification; 2. functional specification and high-level design; 3. high-level design and the low-level design; and 4. low-level design and implementation representation subset.	Provides the following two dimensional mappings: 1. TSS and functional specification; 2. functional specification and high-level design.

Item	Component	Evidence Requirements	How Satisfied	Rationale
7	AGD_ADM.1	Administrator Guidance	Content Server Installation Guide V5.3 Content Server Administrator's Guide V5.3 EMC Documentum Administrator User Guide V5.3 Content Server Fundamentals V5.3 Content Server API Reference Manual V5.3 Content Server DQL Reference Manual, Version 5.3 March 2005	Describes how to administer the TOE securely.
8	AGD_USR.1	User Guidance	EMC Documentum Administrator User Guide V5.3 Content Server Installation Guide V5.3 Content Server Administrator's Guide V5.3 Content Server Fundamentals V5.3 Content Server API Reference Manual V5.3 Content Server DQL Reference Manual, Version 5.3 March 2005	Describes the secure use of the TOE.
9	ATE_COV.1	Test Coverage Analysis	EMC Documentum Content Server V 5.3 and EMC Documentum Administrator V5.3 Test Coverage Analysis V2.1 July, 20 2005	Shows correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.
10	ATE_FUN.1	Test Documentation	DA Common Criteria Test Evidence.Doc	Test documentation includes test plans and procedures and expected and actual results.
11	ATE_IND.2	TOE for Testing	TOE for Testing	The TOE will be provided for testing.
12	AVA_SOF.1	SOF Analysis	EMC Documentum Content Server V 5.3 and EMC Documentum Administrator V5.3 Vulnerability Analysis, Version 1.0 Final, August 23, 2005	Provides a rationale that each mechanism identified in the ST as having an SOF meets or exceeds the minimum strength level specified there.

Item	Component	Evidence Requirements	How Satisfied	Rationale
13	AVA_VLA.1	Vulnerability Analysis	EMC Documentum Content Server V 5.3 and EMC Documentum Administrator V5.3 Vulnerability Analysis, Version 1.0 Final, August 23, 2005	Provide an analysis of the TOE deliverables for obvious ways in which a user can violate the TSP, including the disposition of obvious vulnerabilities.

8.4 PP Claims Rationale

Not applicable. There are no PP claims.

9 Appendix

Table 9-1 Acronyms

ACL	Access Control List
ACM	Configuration Management
ADO	Delivery and Operation
ADV	Development
AES	Advanced Encryption Standard, FIPS PUB 197
AGD	Guidance Documents
ALC	Life cycle support
ATE	Tests
AVA	Vulnerability assessment
CC	Common Criteria [for IT Security Evaluation]
CCIMB	Common Criteria Interpretations Management Board
DBMS	Database Management System
EAL	Evaluation Assurance Level
FAU	Security Audit
FDP	User Data Protection
FIA	Identification and Authentication
FMT	Security Management
FPT	Protection of the TSF
FTA	TOE Access
FTP	Trusted Channels/Path
GUI	Graphical User Interface
ID	Identifier
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
OS	Operating System
PP	Protection Profile
RDBMS	Relational Database Management System
SHA-1	Secure Hash Algorithm Revision 1
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
UI	User Interface

Table 9-2 Terminology

cabinet	The highest level of file storage in a repository is the repository's cabinets. Each cabinet contains folders or categories, and files.
content	*Content* relates to what the object contains or is about, and is *intrinsic* to an information object. This is the data stored.
Content object	When you create or import a file into a repository, EMC Documentum Administrator creates a *content object* that stores two types of information for the file: • The file's content, which is the text, graphics, sound, or video that makes up the file. • The file's properties, which are descriptive characteristics about the file, such as creation date, author, version number, and other information.
folder	Folders are a subset of a cabinet.
metadata	Metadata is data about data. A piece of metadata contains information about a specific information *structure*, irrespective of whatever individual data fields that may comprise that structure. Metadata is the sum total of what can be said about any *information object* at any level of aggregation. In this context, an information object is anything that can be addressed and manipulated by a human or a system as a discrete entity. The object may be comprised of a single item, or it may be an aggregate of many items.[1] The metadata is attributes of the content data. For example, the metadata of a typical document includes the following information: author, subject of document, time it is created.
repository	The repository is called DocBase. This is the storage repository for both content data and metadata. Each repository contains one repository config object. The repository config object defines the name of the underlying RDBMS, security levels for the repository, whether folder security is enabled, and other operating configuration parameters.
Type object	A type object stores structural information about an object type in the Docbase.
SysObject	The SysObject type is the parent type of the most commonly used objects in the EMC Documentum system.
SysObject subtype	The SysObject subtype has a child relationship to a parent type of the most commonly used objects in the EMC Documentum system.

Table 9-3 References

CCITSE	*Common Criteria for Information Technology Security Evaluation*, CCIMB-2004-01-002, Version 2.2, January 2004.
Content_Server_5.3_installation.pdf	Content Server Installation Guide V5.3
Content_Server_5.3_administration.pdf	Content Server Administrator's Guide V5.3
UserGuide.pdf	EMC Documentum Administrator User Guide V5.3
Content_Server_5.3_fundamentals.pdf	Content Server Fundamentals V5.3
Content_Server_5.3_api_reference.pdf	Content Server API Reference Manual V5.3

[1] "Setting the Stage" article by Anne J Gilliland-Swetland