Xacta IA Manager™ Enterprise Edition V4.0 SP2, Build 485

Security Target V1.15

Debra Baker

December 08, 2004

CYGNACOM SOLUTIONS

Suite 5200 ♦7925 Jones Branch Drive♦McLean, VA 22102-3321♦703 848-0883♦Fax 703 848-0960

Revision History:

Date:	Version:	Author:	Description
12/19/2003	0.1	Debra Baker	First Draft
2/1/2004	0.2	Debra Baker	Updates from Vendor
2/2/2004	0.3	Debra Baker	Updates from Vendor
2/5/2004	1.0	Debra Baker	Ready for NIAP
2/6/2004	1.1	Debra Baker	Ready for NIAP
2/18/2004	1.2	Debra Baker	Consistency updates throughout
2/27/2004	1.3	Debra Baker	Consistency updates throughout
3/8/2004	1.4	Debra Baker	Few updates as per Lon
4/20/2004	1.5	Debra Baker	Few updates as per Validator
4/29/2004	1.6	Debra Baker	Updates throughout
5/11/2004	1.7	Debra Baker	Updates throughout per Evaluator
6/9/2004	1.8	Debra Baker	Updates throughout per Evaluator
7/7/2004	1.9	Debra Baker	Updates throughout per Evaluator
8/5/04	1.10	Debra Baker	Updates to cryptographic functions based on the FSP
8/23/04	1.11	Lon Berman and Debra Baker	Updates for change of product name by Vendor. Additional updates provided by ST author
8/26/04	1.12	Lon Berman and Debra Baker	More updates for change of product name by Vendor and ST author
11/3/04	1.13	Debra Baker	Update to FIA_SOS.1
12/1/04	1.14	Debra Baker	Small updates throughout per Evaluator
12/8/04	1.15	Debra Baker	Removed FPT_SEP.1 and FAU_STG.1

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: Xacta IA Manager Enterprise Edition V4.0 SP2, Build 485

ST Title: Xacta IA Manager Enterprise Edition V4.0 SP2, Build 485 Security Target

ST Version: Version 1.15

ST Authors: Debra Baker

ST Date: December 8, 2004

Assurance Level: EAL2

Strength of Function: SOF-basic

Registration: <To be filled in upon registration>

Keywords: Access Control, Identification, Authentication, Security Target, Publishing, and Security Management

1.2 Security Target Overview

This Security Target (ST) defines the Information Technology (IT) security requirements for Xacta IA Manager Enterprise Edition V4.0 SP2, also known as the Xacta Assessment Engine. Xacta IA Manager Enterprise Edition is an information security risk management software application. With Xacta IA Manager Enterprise Edition, you simply define the network or system configuration and the environment in which it operates, and the application automatically engages the appropriate security requirements according to government and/or industry best practices. The software then automatically generates the appropriate test procedures, processes the test results, produces a risk assessment, and allows the user to automatically publish a complete C&A package, including all appendices, in accordance with the National Institute of Standards and Technology (NIST), the Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP), the National Information Assurance Certification and Accreditation Process (NIACAP), or the Director of Central Intelligence Directive (DCID). Through the software's automation of these formal processes, organizations can validate their compliance to Government mandates, such as the Federal Information Security Management Act, Health Insurance Portability and Accountability Act, Gramm-Leach-Bliley Act, and the Privacy Act of 1974. In addition to traditional security assessment and compliance, the software provides Continuous Assessment of the network and system security posture to ensure emerging threats are mitigated prior to an attack.

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.

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, 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.

Acronym definitions and references are provided in sections 9 and 10.

2 TOE DESCRIPTION

2.1 Product Type

Xacta IA Manager Enterprise Edition is an information security risk management software application. With Xacta IA Manager Enterprise Edition, you simply define the network or system configuration and the environment in which it operates, and the application automatically engages the appropriate security requirements according to government and/or industry best practices. The software then automatically generates the appropriate test procedures, processes the test results, produces a risk assessment, and allows the user to automatically publish a complete C&A package, including all appendices, in accordance with the National Institute of Standards and Technology (NIST), the Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP), the National Information Assurance Certification and Accreditation Process (NIACAP), or the Director of Central Intelligence Directive (DCID). Through the software's automation of these formal processes, organizations can validate their compliance to Government mandates, such as the Federal Information Security Management Act, Health Insurance Portability and Accountability Act, Gramm-Leach-Bliley Act, and the Privacy Act of 1974. In addition to traditional security assessment and compliance, the software provides Continuous Assessment of the network and system security posture to ensure emerging threats are mitigated prior to an attack.

2.2 Xacta IA Manager Enterprise Edition Components

Xacta IA Manager Enterprise Edition is comprised of an application server, a publishing server, a Detect Server, and a graphical user interface. A web services engine hosts the application server, and the web services engine is not part of the TOE.

2.2.1 Application Server

The Application Server provides the core business logic of the application. As such, all other Xacta IA Manager Enterprise Edition components communicate with the Application Server. The application server performs the following security functions:

- Identification: application account holders are presented via the Graphical User Interface and validated against account records maintained in the database.
- Authentication: passwords for account holders are presented via the Graphical User Interface, hashed by the application server, and the hash is compared to account password records maintained in the database.
- Access Control: authorised account holders are restricted to projects to which they have been explicitly assigned.
- Authorization: authorised account holders having varying privilege levels that control overall functionality for the following account types: Built-In Master Administrator, Administrator, Executive, User.
- Audit: the Application Server generates an audit trail and stores it in the database (and writes overflow records to the host file system).

The application server can technically be described as business logic that executes inside a web services engine (Apache Tomcat).

2.2.2 Graphical User Interface

Xacta IA Manager Enterprise Edition has a web based graphical user interface through which all Xacta IA Manager Enterprise Edition functions are managed. This same interface is used by all account holders for both administration purposes and for end-user product usage. In any case, users

access the Graphical User Interface via a standard web browser, such as Internet Explorer or Netscape Communicator. Technically, the GUI consists of server-side application software.

2.2.2.1 Administrator Interface

Xacta IA Manager Enterprise Edition has a web based graphical user interface through which all Xacta IA Manager Enterprise Edition functions are managed. A primary function of the application administrator is to create security assessment “projects”, create “user” accounts for persons who will work on those projects, and assign the users to the appropriate projects (based on a project role). As a way of managing or grouping accounts and projects, the administrator has the option to segregate these accounts and projects objects into “folders”. Security policy settings for usernames and passwords are established through the GUI. Also, administrators use the GUI to enable or disable audit logging and to review and archive the audit trail. The Built-in Master Administrator and Administrator accounts use the administrator Interface.

2.2.2.2 User Interface

Normal user login results in the presentation of a list of projects to which a user has been assigned. The user’s access to projects is based on their assignment to specific project roles within a project. (More than one user may be assigned to any particular role within a project.) The primary functions a user executes within the application include the following tasks:

- Requirements & Definition: the user describes the security boundary of a particular automated information system (AIS) and identifies the security requirements that it will be evaluated against
- Inventory & System Information: the user identifies all components within the system boundary and provides other detailed project information
- Vulnerability Assessment & Testing: the user completes checklists, prepares test plan documentation, and enters test results
- Analysis and Reporting: the user performs in-depth analysis of risks identified for the system and completes required deliverable documentation.

Each of these tasks is executed through a series of process steps. Based on the particular role to which a user has been assigned, not all of these tasks will be visible (or accessible). The arrangement of “Tasks” and “Process Steps” within any project is customizable and may vary from one project to the next. (Customers may also define agency-specific workflows and disseminate these in the form of a project template.) Both the Executive and User accounts use the User Interface.

2.2.3 Publishing Server

The publishing server produces either Adobe portable document format (PDF) or Microsoft Word format files. These files are an essential part of the formal work product associated with security certification and accreditation efforts. The user can click the Publish button for any of the system security documents or appendices to begin the publishing process. The application displays the Publishing Status for each section and appendices of the documentation package (i.e., Never Published, Submitted, Start Publishing, and Completed). In addition, you can print classification markings in the header/footer based on a drop-down selection of a number of optional "Document Markings". Currently, the selectable options are For Official Use Only, Confidential, Secret, and Top Secret. Another publishing option is where to put this marking; it's called "Document Marking Location". Its options are Header and Footer, Header Only, and Footer Only. The Publishing Server provides no security services and communicates only with the Application Server.

2.2.4 Detect Server

The Xacta Detect Server is a Java-based scanning utility that utilizes standard network scanning technologies to perform its job. Capabilities provided by the Detect Server include the following:

- Discovery Scanning: discovery and identification of network-connected Information Technology (IT) assets
- Vulnerability Scanning: network-based scanning for known vulnerabilities over a defined Internet Protocol address space
- Collection: polling and information retrieval from Xacta Detect Host Agents that are distributed in the target customer environment. Also, the collection function provides connectivity to and retrieval from enterprise information resources, specifically Tivoli, MS-SMS, and ISS SiteProtector.

The Application Server sends requests and instructions to the Detect Server. The application's Continuous Assessment feature allows network discovery, vulnerability, and collection scans to be scheduled for periodic recurrence. The Detect Server does not have any security functionality. All security functions are implemented by the application server. The same Administrator interface that is used for the Application Server is used for the operation of the Detect Server. All network traffic between the Detect Server and the Detect Host Agents is secured by SSL.

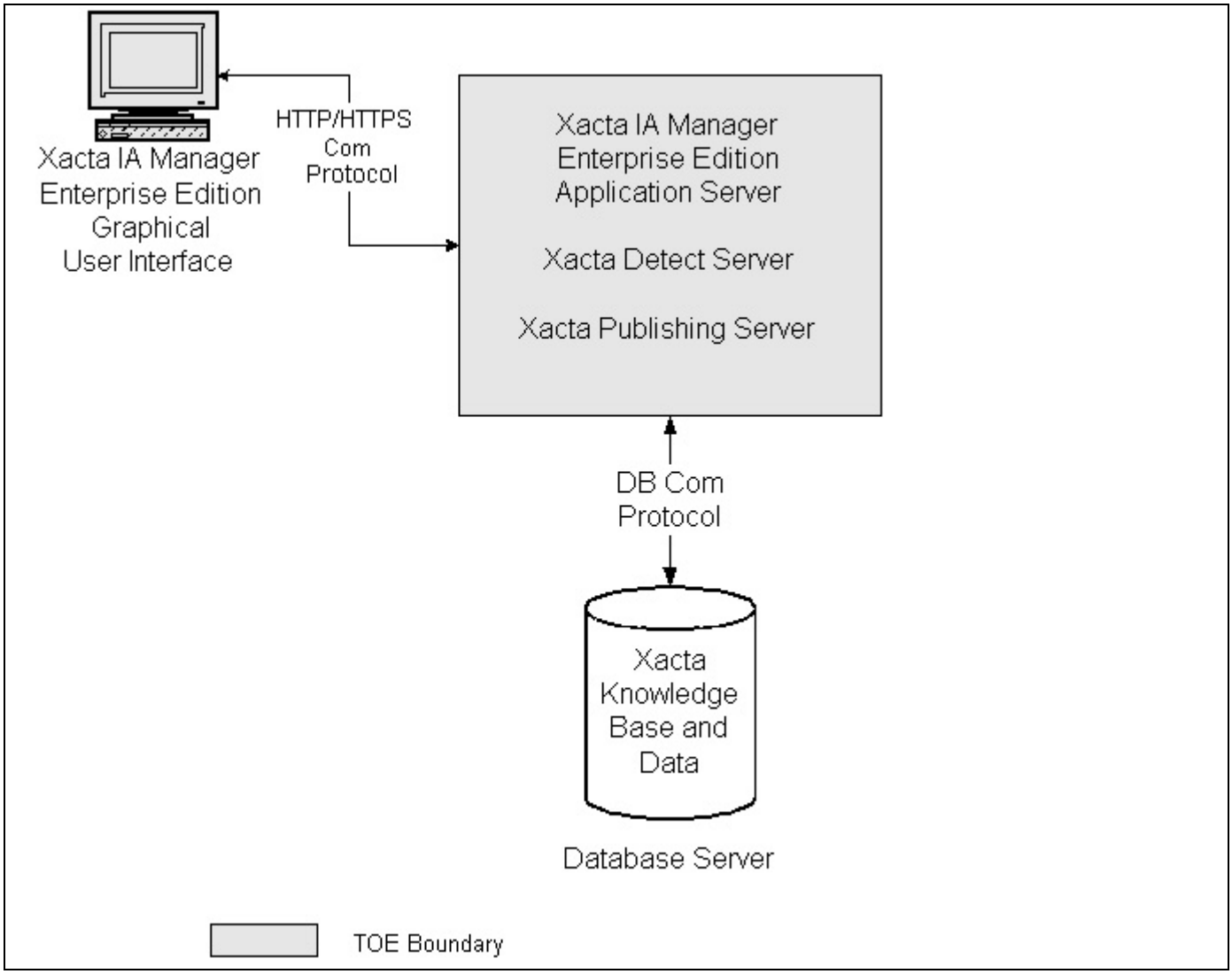

Figure 2-1 Xacta IA Manager Enterprise Edition Architecture Diagram

2.3 TSF Physical Boundary and Scope of the Evaluation

The evaluated configuration will be on a single server deployment that includes the following:

- Xacta IA Manager Enterprise Edition Publishing, Application, Detect Servers and Graphical User Interface running on Windows 2000 Server on the same physical machine. One configuration will have the XIAM-EE Graphical User Interface being presented via Internet Explorer direct from this server.
  - The following software is installed on the Xacta IA Manager Server machine, but is not part of the TOE:
    - Windows 2000 Server
    - Internet Explorer 6.0
    - Web services GUI is a JSP/Servlet application that is executed with a Tomcat 4.0.6.

        - Oracle 9i server/8i client is also installed on this physical machine for data management.
        - Java Runtime Environment (JRE) version j2sdk1.4.2
        - MSOffice 2000 (MSWord and MSExcel)
        - Acrobat Reader

- The XIAM-EE Graphical User Interface will also be presented on a separate machine running Internet Explorer 6.0 on a Windows 2000 workstation. There are no TOE components installed on the workstation.
    - The following software is installed on the separate workstation machine but is not part of the TOE:
        - Windows 2000 workstation
        - Internet Explorer 6.0
        - MSOffice 2000 (MSWord and MSExcel)
        - Acrobat Reader

The evaluated configuration will have the Xacta IA Manager Enterprise Edition configured so that the built-in Master Administrator account's remote login capability is disabled. The TOE includes the Xacta IA Manager Enterprise Edition publishing server, application server, detect server and the graphical user interface. The Xacta Detect Host Agent is a separate software package that is not included in the TOE. In addition, the underlying operating system (OS) software and hardware are not part of the TOE. The third party relational database is not included in the TOE. The interface of the third party database in not included as part of the TOE. The TOE also does not include the third-party encryption software that is used to provide a trusted communication path between users and the TOE or applications used to view TOE output (MS Word, MS Excel, Adobe Acrobat).

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 section 5 and 6. Xacta IA Manager Enterprise Edition provides the following security features:

- **Security audit** - Xacta IA Manager Enterprise Edition provides its own auditing capabilities separate from those of the Operating System. Xacta IA Manager Enterprise Edition provides the ability to search, sort, order, and view its own audit records.
- **User data protection** - Xacta IA Manager Enterprise Edition provides its own complete access control separate from the Operating System between subjects and objects covered by the Xacta IA Manager Enterprise Edition Access Control Policy (see Table 5-3).
- **Identification and authentication** - Xacta IA Manager Enterprise Edition provides user identification and authentication through the use of user accounts and the enforcement of password policies.
- **Security management** - Xacta IA Manager Enterprise Edition provides security management through the use of the Administrator Interface. Through the enforcement of the Xacta IA Manager Enterprise Edition Access Control Policy, the ability to manage various security attributes is controlled.

2.5 TOE Security Environment

It is assumed that there will be no untrusted users or software on the Xacta IA Manager Enterprise Edition Server host. Xacta IA Manager Enterprise Edition relies upon the underlying operating system and platform to provide reliable time stamps and to protect the Xacta IA Manager Enterprise Edition Server host from other interference or tampering. Xacta IA Manager Enterprise Edition relies on a Web Server to provide web services. The TOE will be deployed on a trusted intranet. The TOE environment is one where the potential attacker is unsophisticated, with access to only standard equipment and public information about the product.

The TOE security environment can be categorized as follows:

- **Cryptographic Support** - The TOE relies on the IT environment to provide cryptographic support. These include:
  - digital signature verification for authentication;
  - encryption for a trusted path to prevent user data disclosure.
  - MD5-based encryption scheme is used for all password encryption.
  - Single DES (Data Encryption Standard) is used for project backup and restoration.
  - Java Cryptography Extension (JCE) algorithm, provided by Sun Microsystems, is used for encoding/decoding zipped XML documents sent between the XWCA application and the Publisher.
  - BASE64 Encoding algorithm, provided by Sun Microsystems, is used for encoding images saved in the XWCA database. This includes images sent to the Publisher from the XWCA application.
- **Trusted Path** - The TOE relies on the IT environment to provide encrypted communications over a trusted path. Trusted path refers to the encrypted connection that prevents disclosure and detects modification of data transmitted between a human user and the TOE, e.g., a remote administration or user connection. The trusted path must be used for any user password-based authentication and all remote administration actions.
- **Relational Database** - The Relational database provides the following:
  - Ensures data security with logins and passwords
  - Capability to store query results and reduce response time with indexed views
  - XML support
  - Audit log storage and retrieval
- **Tomcat 4.0.6 Servlet Engine** -
  - Supports both unsecured HTTP and secured HTTPS (SSL) connections.
  - Supports authentication via certificates
  - Servlet context
- **Operating System and Hardware** –

The OS and Hardware is being relied on for protection and execution of the software, disk storage, and reliable time stamps.

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.

A.Access	It is assumed that only authorized TOE, database, and operating system administrators have access to the data stored in the database and the underlying operating system.
A.Admin	The administrator is trusted to correctly configure and operate the TOE according to the instructions provided by the TOE documentation.
A.Intranet	It is assumed that the Xacta IA Manager Enterprise Edition Server is deployed on a trusted intranet.
A.Manage	It is assumed that one or more authorised administrators are assigned who are competent to manage the TOE and the security of the information it contains, and who can be trusted not to deliberately abuse their privileges so as to undermine security.
A.NoUntrusted	It is assumed that there will be no untrusted users and no untrusted software on the Xacta IA Manager Enterprise Edition Server host.
A.Physical	The TOE components critical to the security policy enforcement will be protected from unauthorized physical modification.
A.Time	It is assumed that the underlying operating system provides reliable time stamps.
A.Users	It is assumed that users will protect their authentication data.

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 is unsophisticated, with access to only standard equipment and public information about the product.

The TOE must counter the following threats to security:

T.Abuse	An undetected compromise of the TOE may occur as a result of an authorised user of the TOE (intentionally or otherwise) performing actions the individual is authorised to perform.
T.Access	An authorised 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.BadPassword	Users may not select good passwords on their own, allowing attackers to guess their passwords and obtain unauthorised access to the TOE.
T.Bypass	An attacker may attempt to bypass TSF security functions to gain unauthorised access to TSF.
T.Mismanage	Authorised administrators may make errors in the management of security functions and TSF data. Administrative errors may allow attackers to gain unauthorised access to resources protected by the TOE.
T.Privil	An unauthorised user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
T.Tamper	An attacker may attempt to modify TSF programs and data.
T.Transmit	TSF data may be disclosed or modified by an attacker while being transmitted between the TOE and its users.
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.Walkaway	A user may leave his workstation without logging out. A user may leave his workstation without logging out thus allowing unauthorized users to gain access to resources and data protected by the TOE.

4 Security Objectives

4.1 Security Objectives for the TOE

The security objectives for the TOE are as follows:

O.Access	The TOE must allow authorised users to access only appropriate TOE functions and data.
O.Admin	The TOE must provide the functionality to enable authorised user(s) to effectively manage the TOE and its security functions.
O.Attributes	The TOE must be able to store and maintain attributes.
O.Audit	The TOE must record audit records for data accesses and use of the TOE functions.
O.IDAuth	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
O.LoginNameQual	The TOE must be able to specify login name minimum length requirements
O.NonBypass	The TOE must ensure the security enforcing functions are invoked and succeed before allowing a TOE function to proceed.
O.PasswordQual	The TOE must be able to specify password quality parameters such as password history, minimum length, and password compositions.
O.ProtectAuth	The TOE will provide protected authentication feedback.
O.Re-authenticate	The TOE must be able to require the user to be re-authenticated after session time-out.
O.Roles	The TOE must support multiple roles.

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:

OE.ProtectComm	The IT environment must protect communications between the TOE and its users.
OE.ProtectData	The IT Environment must protect passwords and project data.
OE.Time	The underlying operating system must provide reliable time stamps.

4.2.2 Security Objectives for Non-IT Security Environment

The Non-IT security objectives are as follows:

ON.Install	Those responsible for the TOE must ensure that the TOE is delivered and installed in a manner that maintains IT security.
ON.NoUntrusted	The administrator must ensure that there are no untrusted users and no untrusted software on the Xacta IA Manager Enterprise Edition Server host.
ON.Operations	The TOE will be managed and operated in a secure manner as outlined in the supplied guidance.
ON.ProtectAuth	Users must ensure that their authentication data is held securely and not disclosed to unauthorised persons.
ON.Person	Personnel working as authorised administrators shall be carefully selected and trained for proper operation of the system.
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.

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 are described. These requirements consist of functional components from Part 2 of the CC, assurance components from Part 3 of the CC, NIAP and International interpretations, and explicit functional components derived from the CC components.

5.1 Formatting 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. 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 International 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.
- *Comments* are provided as an aid to the ST author and evaluation team. These items will be deleted in the final version of the ST.

5.2 TOE Security Functional Requirements

The functional security requirements for the TOE consist of the following components derived from Part 2 of the CC and explicit components, summarized in the Table 5-1 below.

Table 5-1 Functional Components

No.	Component	Component Name
1.	FAU_GEN.1	Audit data generation
2.	FAU_GEN.2	User identity association
3.	FAU_SAR.1	Audit review
4.	FAU_SAR.2	Restricted audit review
5.	FAU_SAR.3	Selectable audit review
6.	FDP_ACC.2	Complete access control
7.	FDP_ACF.1	Security attribute based access control
8.	FIA_AFL.1	Authentication failure handling
9.	FIA_ATD.1	User attribute definition
10.	FIA_SOS.1	Verification of secrets
11.	FIA_SOS_EXP.1	Verification of login names
12.	FIA_UAU.2	User authentication before any action
13.	FIA_UAU.6	Re-authenticating
14.	FIA_UAU.7	Protected authentication feedback
15.	FIA_UID.2	User identification before any action
16.	FMT_MOF.1	Management of Security Functions Behavior
17.	FMT_MSA.1	Management of security attributes
18.	FMT_MSA.3	Static attribute initialisation
19.	FMT_MTD.1	Management of TSF data
20.	FMT_SMF.1	Specification of management functions
21.	FMT_SMR.1	Security roles
22.	FPT_RVM.1	Non-bypassability of the TSP
23.	FTA_TAB.1	Default TOE access banners

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 see column 1 in Table 5-2:

Table 5-2 Audit Events and Persistent Classes

Audit Event	Persistent Classes
Application Settings Changed	
• Account Login	○ Account

Audit Event	Persistent Classes
• Account Login Failure • Account Logout • Account Forced Logoff • Security Policy Change	
• Security Policy Change	○ User
• Creation • Update • Deletion	○ Account ○ Acronym ○ Alert ○ Alert.Associated ○ AlertScheduler ○ Appendix ○ Application ○ Assignment ○ AutomatedTest ○ Barrel ○ Bucket ○ Checklist ○ CheckListEntry ○ CheckListGroup ○ CheckListQuestion ○ CheckListQuestion.Answer ○ ChoiceOption ○ Component ○ ContentScheduler ○ Criteria ○ Criteria.Status ○ Definition ○ DetectConfig ○ DetectConstraints ○ DetectScan ○ DetectScanConfig ○ DetectScanStatus ○ DetectSegment ○ Document ○ DocumentFigure ○ DocumentIncluded ○ DocumentReference ○ Equipment ○ Equipment.SET_Application ○ Equipment.SET_Vulnerability ○ EquipmentGroup ○ EquipmentProperty ○ Folder ○ Help ○ Location ○ Location.SET_Threats

Audit Event	Persistent Classes
	○ Lookup ○ Matcher ○ Milestone ○ OptionList ○ Os ○ Permission ○ Prereq ○ Project ○ ProjectAttributes.Data ○ ProjectHead ○ ProjectPersonnel ○ PStep ○ Reference ○ Regulation ○ ReqCriteria ○ Requirement ○ Requirement.SET_Tests ○ Requirement.Status ○ RiskElement ○ RiskLevel ○ RiskSnapshot ○ Role ○ SampleDoc ○ ScheduleElement ○ Softwae ○ SSAA ○ SysDataFlow ○ SysInterface ○ SystemUser ○ Test ○ TestProc ○ Threat ○ TimerEvent ○ User ○ Wp ○ Wp.SET_Psteps ○ WpState

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: **[*affected project*]**

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 **[*the authorised administrator*]** with the capability to read **[*all audit information within the administrator's scope of control (See Table 5-3)*]** 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, sorting, and ordering*]** of audit data based on **[*time stamp, user, project, events, and description of audit event*]**.

Dependencies: FAU_SAR.1 Audit review

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 **[*Table 5-3 Xacta IA Manager Enterprise Edition Access Control Policy*]** on **[*Subjects and Objects listed in Table 5-3*]** 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

Table 5-3 Xacta IA Manager Enterprise Edition Access Control Policy

Level of Access	Subjects holding the following types of accounts:	Description of Access	Objects:
Site-Level	Built-In Master Administrator	Full Access privileges The Built-in Master Administrator Account has access to all information in the application and is the only account that can configure the System Settings. Note: System Settings are included in application settings and security policy functions.	• Accounts • Configure (Policies, System Settings, Continuous Assessment Settings, System of System Configuration) • Folders • Projects • Reports
	Administrator	Full Access privileges except cannot configure System Settings. Access, modify, or configure your organization's projects and continuous assessment settings. Site-level administrators also have access to system-of-systems reports via the applications reporting function.	• Accounts • Configure (Continuous Assessment Settings, System of System Configuration) • Folders • Projects • Reports
	Executive	Full read-only access privileges. Executive accounts should be assigned only to those who have a need to view all of your organization's projects. Site-level executives also have access to system-of-systems reports via the application's reporting function.	• Accounts • Folders • Projects • View (Continuous Assessment Settings, System of System Settings) • Reports
	User	Although a site-level user can be assigned to any project contained in the application, he or she can access only those projects to which he or she is assigned. Assignments to projects are based on roles defined within each project; this further restricts access within each project. User accounts designated as project administrator's can define project roles and assign users to project roles.	• Projects

Level of Access	Subjects holding the following types of accounts:	Description of Access	Objects:
Folder-Level	Administrator	Administrators have read/write access to all projects contained in their assigned folders. Folder-level administrators also have access to reports via the application's reporting features.	• Accounts • Configure (Continuous Assessment Settings, System of System Configuration) • Projects • Reports
	Executive	Executives have read-only access to all projects contained in their assigned folders. Folder-level executives also have access to reports via the application's reporting function.	• Accounts • Projects • View (System of System Settings) • Reports
	User	Although a folder-level user can be assigned to any project contained in his or her folder, he or she can only access those projects to which he or she is assigned. Assignments to projects are based on roles defined within each project; this further restricts access within each project. User accounts designated as project administrators can define project roles and assign users to project roles within their scope of control.	• Projects • Set (Continuous Assessment Settings)

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1 The TSF shall enforce the **[*Table 5-3 Xacta IA Manager Enterprise Edition Access Control Policy*]** to objects based on the following: **[*Subjects with Account Type Attribute and Objects listed in Table 5-3*]**.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[*see Table 5-3*]**.

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 explicit deny rules*]**.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

5.2.3 Class FIA: Identification and Authentication

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

FIA_AFL.1.1 The TSF shall detect when **[*an administrator configured maximum number of*]** unsuccessful authentication attempts occur related to **[*administrator, executive, and user login attempts*].**

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall **[*disable the administrator, executive, and user accounts until the account is reactivated by an authorised account holder*].**

Application Note: By design, the built-in master administrator account is never deactivated.

Dependencies: FIA_UAU.1 Timing of 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:

- **[*Account Name;***
- ***Account Type user can assume (listed in column 2 of Table 5-3);***
- ***Password;***
- ***Active/Inactive State;***
- ***Assigned Folder(s);***
- ***Account Disabled Date;***
- ***Password Expiration;***
- ***Password History;***
- ***Assigned Project(s) if any;***
- ***Project Role(s) if any*]**

Dependencies: No dependencies.

FIA_SOS.1 Verification of secrets

Hierarchical to: No other components.

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet **[*the rules of the password policy (See Table 5-4)*]**

Table 5-4 Password Policy Rules

Rule	Description
Minimum Alpha	Minimum number of alphabetic characters is 6
Minimum Numeric	Minimum number of numeric characters is 2.
Password Expiration	Maximum number of days before a password must be changed.
Password History Policy	Number of previous passwords to be checked against new passwords.
Minimum Password Length	Minimum number of characters required is 8 in all passwords.

Dependencies: No dependencies.

FIA_SOS_EXP.1 Verification of login names
Hierarchical to: No other components.

FIA_SOS_EXP.1.1 The TSF shall provide a mechanism to verify that the login name meet the minimum number of characters required is 8 in all login names.

Dependencies: No dependencies.

FIA_UAU.2 User authentication before any action
Hierarchical to: FIA_UAU.1

FIA_UAU.2.1 The TSF 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

FIA_UAU.6 Re-authenticating
Hierarchical to: No other components.

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions **[*configurable session time out]***.

Dependencies: No dependencies.

FIA_UAU.7 Protected authentication feedback
Hierarchical to: No other components.

FIA_UAU.7.1 The TSF shall provide only **[*a display of the typed in user name and asterisks for the password for password-based authentication*]** to the user while the authentication is in progress.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UID.2 User identification before any action
Hierarchical to: FIA_UID.1

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

Dependencies: No dependencies.

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 **[*audit (see FAU_GEN.1.1)*]** to **[*the Built-In Master Administrator*]*.***

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MSA.1 Management of security attributes
Hierarchical to: No other components.

FMT_MSA.1.1 The TSF shall enforce the **[*Table 5-3 Xacta IA Manager Enterprise Edition Access Control Policy*]** to restrict the ability to **[*query, modify, delete,* [*clear, and create*] *as specified in Table 5-5*]** the security attributes **[*as specified in Table 5-5*]** to **[*the role as specified in Table 5-5*]**.

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

Table 5-5 Management of Security Attributes

Level Of Access	Account Types	Allowed Action on Specified Security Attributes
Site-level	Built-In Master Administrator	• Modify account disable date • Create and modify the site-level password policy • Modify password expiration • Create, query, modify, and delete the account name, assigned folder, assigned project, assigned project role, account type, and active/inactive state • Clear the password history of a selected account
	Administrator	• Modify account disable date • Modify password expiration • Create, query, modify, and delete the account name, assigned folder, selected policy, assigned project, assigned project role, account type, and active/inactive state • Clear the password history of a selected account
	User assigned as Project Administrator	• Create, query, modify, and assign project roles • Assign user to a project by assigning the user to a role associated with a project
Folder-level	Administrator	• Modify account disable date • Modify password expiration • Create, query, modify, and delete account name, assigned project, assigned project role, account type, and active/inactive state. • Clear the password history of a selected account
	User assigned as Project Administrator	• Create, query, modify, and assign project roles within his/her assigned projects • Assign user to a project by assigning the user to a role associated with a project

FMT_MSA.3 Static attribute initialisation
Hierarchical to: No other components.

FMT_MSA.3.1 The TSF shall enforce the **[*Table 5-3 Xacta IA Manager Enterprise Edition Access Control Policy*]** to provide **[*restrictive*]** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the **[*Built-in Master Administrator, Site-Level administrator, and Folder-Level administrator*]** 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 **[*change_default, query, modify, delete, clear, [list, sort, view, archive, and create]] as specified in Table 5-6*]** the **[*TSF Data as specified in Table 5-6*]** to **[*the role as specified as account types in Table 5-6*]*.***

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

Table 5-6 Management of TSF Data

Level of Access	Account Types	Allowed Operations on TSF Data (Management Functions)
Site-Level	Built-In Master Administrator	The Built-In Master Administrator can: • query, create, modify, and delete site-level and folder-level administrator, executive, and user accounts at site level and in folders • access to query, modify, and force logoff of on-line user accounts • query, create, modify, archive, and delete site-level and folder-level projects; assign users to projects • query, create, modify, and delete all folders • view, clear, and export all the audit logs • query, create, modify, and delete project roles; assign users to project roles
	Administrator	The site-level administrator can: • query, create, modify, and delete site-level and folder-level administrator, executive, and user accounts at site level and in folders • access to query, notify, and force logoff of on-line user accounts • query, create, modify, archive, and delete projects; assign users to projects • query, create modify, and delete folders • view and export all the audit logs • query, create, modify, and delete project roles; assign users to project roles

Level of Access	Account Types	Allowed Operations on TSF Data (Management Functions)
	Executive	The site-level executive can: • query and view all accounts • query and view all projects • query and view all folders • query and view all project roles • list/sort and notify on-line user accounts
	User	The site-level user can access only those projects to which he or she is assigned. The site-level user assigned the role of a project administrator can define project roles and assign users to project roles within his / her scope of control. A site-level user assigned the role of a project administrator can: • create, query, modify, and assign project roles • assign user to a project by assigning the user to a role associated with a project
Folder-Level	Administrator	Within the folder-level scope of control administrators can: • query, create, modify, and delete administrator, executive, and user accounts within their assigned folder • query, create, modify, and delete projects • query, create, modify, archive, and delete project roles within the assigned folder • assign users to projects within the assigned folder by associating the user with a project role • view and export the folder-level audit logs
	Executive	Within the folder-level scope of control executives can: • query and view accounts within the assigned folder • query and view projects within the assigned folder • review folders • query and view project roles within the assigned folder
	User	Within the folder-level scope of control, users can access only those projects to which he or she is assigned. The folder-level user assigned the role of project administrator can define project roles and assign users to project roles within his/her scope of control. A site-level user assigned the role of a project administrator can: • create, query, modify, and assign project roles • assign user to a project by assigning the user to a role associated with a project

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 audit (see FAU_GEN.1.1) (see FMT_MOF.1),***
- ***query, modify, delete, and create the security attributes as specified in Table 5-5 (see FMT_MSA.1),***
- ***change_default, query, modify, delete, clear and create as specified in Table 5-6 and the TSF Data as specified in Table 5-6 (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 **[*see account types identified in column 2 of Table 5-3 Xacta IA Manager Enterprise Edition Access Control Policy*].**

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.1 Non-bypassability of the TSP

Hierarchical to: No other components.

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

Dependencies: No dependencies.

5.2.6 Class FTA: TOE access

FTA_TAB.1 Default TOE access banners

Hierarchical to: No other components.

FTA_TAB.1.1 Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorised use of the TOE.

Dependencies: No dependencies.

5.2.7 Strength of Function

The overall strength of function requirement is SOF-basic. The strength of function requirement applies to FIA_SOS.1 and FIA_SOS_EXP.1. The SOF claim for FIA_SOS.1 and FIA_SOS_EXP.1 is SOF-basic. The strength of the “secrets” mechanism is consistent with the objectives of authenticating users (O.IDAuth). In addition, O.PasswordQual is consistent with the SOF-basic claim. Strength of Function shall be demonstrated for the non-certificate based authentication mechanisms to be SOF-basic, as defined in Part 1 of the CC. Specifically, the local authentication mechanism must demonstrate adequate protection against attackers possessing a low-level attack potential.

5.3 Security requirements for the IT Environment

Xacta IA Manager Enterprise Edition requires that the operating system platform provide reliable time stamps. Xacta IA Manager Enterprise Edition requires that the operating system provides TSF domain separation. All cryptographic functions are part of the IT environment, not part of the TOE.

Table 5-7 Functional Components for the IT environment

No.	Component	Component Name
1.	FCS_CKM.1	Cryptographic key generation
2.	FCS_CKM.4	Cryptographic key destruction
3.	FCS_COP.1*	Cryptographic operation
4.	FMT_MSA.2	Secure security attributes
5.	FPT_STM.1	Reliable time stamps
6.	FTP_TRP.1	Trusted Path

5.3.1 Class FCS: Cryptographic Support

FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

FCS_CKM.1.1 **Refinement:** The ***IT environment*** shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[*DES*]** and specified cryptographic key sizes **[*56 bit*]** that meet the following: **[*Data Encryption Standard (DES), FIPS PUB 46-3*]**.

Dependencies: [FCS_CKM.2 Cryptographic key distribution or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

FCS_CKM.4.1 **Refinement:** The ***IT environment*** shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **[*which zeroizes all plaintext cryptographic keys*]** that meets the following: **[*none*]**.

Dependencies: [FDP_ITC.1 Import of user data without security attributes or
FCS_CKM.1 Cryptographic key generation]
FMT_MSA.2 Secure security attributes

FCS_COP.1-1 Cryptographic operation

Hierarchical to: No other components.

FCS_COP.1.1-1 **Refinement:** The ***IT environment*** shall perform **[*symmetric key encryption and decryption*]** in accordance with a specified cryptographic algorithm **[*DES*]** and cryptographic key sizes **[*56 bit*]** that meet the following: **[*Data Encryption Standard (DES), FIPS PUB 46-3*]**.

Dependencies: [FDP_ITC.1 Import of user data without security attributes or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

FCS_COP.1-2 Cryptographic operation

Hierarchical to: No other components.

FCS_COP.1.1-2 **Refinement:** The ***IT environment*** shall perform **[*hashing functions*]** in accordance with a specified hashing algorithm **[*MD5*]** and cryptographic key sizes **[*128 bit hash value*]** that meet the following: **[*Vendor Affirmed*]**.

Dependencies: None

5.3.2 Class FMT: Security Management

FMT_MSA.2 Secure security attributes

Hierarchical to: No other components.

FMT_MSA.2.1 **Refinement:** The ***IT environment*** shall ensure that only secure values are accepted for security attributes.

Dependencies: ADV_SPM.1 Informal TOE security policy model
[FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

5.3.3 Class FPT: Protection of the TOE Security Functions

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

5.3.4 Class FTP: Trusted path/channels

FTP_TRP.1 Trusted path

Hierarchical to: No other components.

FTP_TRP.1.1 **Refinement:** The ***IT environment*** shall provide a communication path between ***the TSF*** and **[*remote and local*]** users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.

FTP_TRP.1.2 **Refinement:** The ***IT environment*** shall permit **[*local users and remote users*]** to initiate communication via the trusted path.

FTP_TRP.1.3 **Refinement:** The ***IT environment*** shall require the use of the trusted path for **[*initial user authentication and* [*all subsequent requests and responses with the TOE*]]**.

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 5-8.

Table 5-8 EAL2 Assurance Components

Component	Component Title
ACM_CAP.2	Configuration items
ADO_DEL.1	Delivery procedures
ADO_IGS.1	Installation, generation, and start-up procedures
ADV_FSP.1	Informal functional specification
ADV_HLD.1	Descriptive high-level design
ADV_RCR.1	Informal correspondence demonstration
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance
ATE_COV.1	Evidence of coverage
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing – sample
AVA_SOF.1	Strength of TOE security function evaluation
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 Xacta Application Server Interface and the Xacta IA Manager Enterprise Edition Graphical User 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 6.1.2, the Xacta Application Server Interface and the Xacta IA Manager Enterprise Edition Graphical User Interface will be mutually referred to as Xacta IA Manager Enterprise Edition.

Table 6-1 Security Functional Requirements mapped to Security Functions

SFRs	Security Class	Security Functions	Sub-functions
FAU_GEN.1	Security audit	Security Audit	SA-1
			SA-2
FAU_GEN.2	Security audit	Security Audit	SA-3
FAU_SAR.1	Security audit	Security Audit	SA-4
FAU_SAR.2	Security audit	Security Audit	SA-5
FAU_SAR.3	Security audit	Security Audit	SA-6
FDP_ACC.2	User data protection	Manage User Access	MUA-1
FDP_ACF.1	User data protection	Manage User Access	MUA-1
FIA_AFL.1	Identification and authentication	Manage User Access	MUA-2
FIA_ATD.1	Identification and authentication	Manage User Access	MUA-3
FIA_SOS.1	Identification and authentication	Manage User Access	MUA-4
FIA_SOS_EXP.1	Identification and authentication	Manage User Access	MUA-5
FIA_UAU.2	Identification and authentication	User Login	UL-1
FIA_UAU.6	Identification and authentication	User Login	UL-2
FIA_UAU.7	Identification and authentication	User Login	UL-3
FIA_UID.2	Identification and authentication	User Login	UL-4
FMT_MOF.1	Security management	Security Management	SM-1
FMT_MSA.1	Security management	Security Management	SM-2
FMT_MSA.3	Security management	Security Management	SM-3
FMT_MTD.1	Security management	Security Management	SM-4
FMT_SMF.1	Security management	Security Management	SM-5
FMT_SMR.1	Security management	Security Management	SM-6
FPT_RVM.1	Protection of the TSF	Manage User Access	MUA-6
FTA_TAB.1	TOE access	User Login	UL-5

6.1.2 Xacta IA Manager Enterprise Edition

Security Function: Security Audit Function	
Sub-function ID	Sub-function description
SA-1	Xacta IA Manager Enterprise Edition generates the following types of audit events: • Startup and shutdown of audit functions • Application Settings Changed • Creation • Update • Deletion • Security Policy Change • Account Forced Logoff • Account Login • Account Login Failure • Account Logout (FAU_GEN.1.1)
SA-2	The following information is recorded for all events: • Date and time of event, • Type of event, • Subject identity, • Description (Success or failure of event), • Affected project. (FAU_GEN.1.2)
SA-3	Xacta IA Manager Enterprise Edition will associate each auditable event with the identity of the user account that caused the event. (FAU_GEN.2)
SA-4	Xacta IA Manager Enterprise Edition provides the built-in master administrator and site-level administrator with the capability to read all audit information in the audit records and in a manner suitable to interpret the information. Xacta IA Manager Enterprise Edition provides the folder-level administrator with the capability to read all audit information within the folder-level administrator's scope of control from the audit records and in a manner suitable to interpret the information. (FAU_SAR.1)
SA-5	Xacta IA Manager Enterprise Edition prohibits all account types read access to the audit records, except administrator's that have been granted explicit read-access. (FAU_SAR.2)
SA-6	Xacta IA Manager Enterprise Edition provides the ability to perform searches, sorting, and ordering of the audit data, based time stamp, user account, project, events, and description of audit event. (FAU_SAR.3)

Security Function: Manage User Access Function	
Sub-function ID	Sub-function description
MUA-1	Xacta IA Manager Enterprise Edition enforces the Xacta IA Manager Enterprise Edition Access Control Policy (See Table 5-3 Xacta IA Manager Enterprise Edition Access Control Policy) (FDP_ACC.2) (FDP_ACF.1)
MUA-2	Xacta IA Manager Enterprise Edition detects when an administrator configured maximum number of unsuccessful authentication attempts occur related to administrator, executive, and user account login attempts. When the defined number of unsuccessful authentication attempts has been met or surpassed, Xacta IA Manager Enterprise Edition disables the administrator, executive, and user accounts until the account is reactivated by an authorised administrator. (FIA_AFL.1) The built-in Master Administrator cannot be locked out. In addition, Xacta IA Manager Enterprise Edition can be configured so that the built-in Master Administrator account cannot be accessed remotely.
MUA-3	Xacta IA Manager Enterprise Edition maintains the following information for each account: account name, account type(s) user can assume (listed in column 2 of Table 5-3), password, active/inactive state, assigned folders, account disabled date, password expiration, password history, assigned project(s), and project roles. (FIA_ATD.1)
MUA-4	Xacta IA Manager Enterprise Edition requires that user account passwords meet the rules of the password policy (See Table 5-4 Password Policy Rules). (FIA_SOS.1)
MUA-5	Xacta IA Manager Enterprise Edition provides a mechanism to verify the login name meets the minimum number of characters required is 8 in all login names (FIA_SOS_EXP.1)
MUA-6	Xacta IA Manager Enterprise Edition ensures that the Table 5-3 Xacta IA Manager Enterprise Edition Access Control Policy is invoked and succeeds before each function is allowed to proceed. (FPT_RVM.1)

Security Function: Security Management Function	
Sub-function ID	Sub-function description
SM-1	Xacta IA Manager Enterprise Edition 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 the Built-In Master Administrator. (FMT_MOF.1)
SM-2	Xacta IA Manager Enterprise Edition restricts the ability to query, modify, delete, clear, and create the specified security attributes (see Table 5-5) to the specified user accounts (see Table 5-5) (FMT_MSA.1)
SM-3	Xacta IA Manager Enterprise Edition enforces the Table 5-3 Xacta IA Manager Enterprise Edition Access Control Policy to provide restrictive default values for security attributes that are used to enforce the SFP. Xacta IA Manager Enterprise Edition allows per the Xacta IA Manager Enterprise Edition Access Control Policy the Built-in Master Administrator, site-level administrator, and Folder-Level administrator to specify alternative initial values. (FMT_MSA.3)
SM-4	Xacta IA Manager Enterprise Edition restricts the ability to access data as specified in Table 5-6 Management of TSF Data. (FMT_MTD.1)

Security Function: Security Management Function	
Sub-function ID	Sub-function description
SM-5	Xacta IA Manager Enterprise Edition provides the following security management functions: • determine the behavior of, disable, enable, and modify the behavior of the functions audit (see FAU_GEN.1.1) (see FMT_MOF.1), • query, modify, delete, and create the security attributes as specified in Table 5-5 (see FMT_MSA.1), • change_default, query, modify, delete, clear and create as specified in Table 5-6 the TSF Data as specified in Table 5-6 (See FMT_MTD.1). (FMT_SMF.1)
SM-6	Xacta IA Manager Enterprise Edition maintains the roles identified in column 2 of Table 5-3 Xacta IA Manager Enterprise Edition Access Control Policy. (FMT_SMR.1)

Security Function: User Login Function	
Sub-function ID	Sub-function description
UL-1	Xacta IA Manager Enterprise Edition requires each user account to successfully authenticate with a password before being allowed any other actions. (FIA_UAU.2)
UL-2	The Xacta IA Manager Enterprise Edition requires the user account to re-authenticate when the session times out. (FIA_UAU.6)
UL-3	The Xacta IA Manager Enterprise Edition provides only a display of the typed in user account name and asterisks for the password when password authentication is used. (FIA_UAU.7)
UL-4	The Xacta IA Manager Enterprise Edition requires each user to identify himself/herself before being allowed to perform any other actions. (FIA_UID.2)
UL-5	The Xacta IA Manager Enterprise Edition requires the TSF to display an advisory warning message regarding unauthorised use of the TOE. (FTA_TAB.1)

6.1.3 SOF Claims

The following IT Security Functions are realized by probabilistic or permutational mechanisms:

- MUA-4: Manage User Access Function for the Administrator Interface
- MUA-5: Manage User Access Function for the Administrator Interface

Within MUA-4, the methods used to provide difficult-to-guess passwords are probabilistic. Within MUA-5, the methods used to provide minimum length for user account names are probabilistic. The SOF claim for all of these IT security functions is SOF-basic.

6.2 Assurance Measures

The Xacta IA Manager Enterprise Edition satisfies the assurance requirements for Evaluation Assurance Level EAL2. The following items are provided as evaluation evidence to satisfy the EAL2 assurance requirements:

Table 6-2 Assurance Measures and How Satisfied

Security Assurance Requirement	How Satisfied
ACM_CAP.2	Configuration Items for Xacta IA Manager Enterprise Edition Version 4.0 SP2 – 01 December 2004

Security Assurance Requirement	How Satisfied
ADO_DEL.1	Delivery Procedures for Xacta IA Manager Enterprise Edition Version 4.0 SP2 – 26 September 2004
ADO_IGS.1	Secure Installation & Configuration Supplement for for Xacta IA Manager Enterprise Edition Version 4.0 SP2 – 03 November 2004
ADV_FSP.1	Security Functional Specification for Xacta IA Manager Enterprise Edition Version 4.0 SP2 – 09 November 2004
	Xacta IA Manager Enterprise Edition Reference Manual – 24 September 2004
ADV_HLD.2	High Level Design for Xacta IA Manager Enterprise Edition Version 4.0 SP2 – 21 August 2004
	Xacta IA Manager Enterprise Edition Reference Manual – 24 September 2004
ADV_RCR.1	Informal Correspondence Demonstration for Xacta IA Manager Enterprise Edition Version 4.0 SP2 – 21 August 2004
AGD_ADM.1	Xacta IA Manager Enterprise Edition Reference Manual – 24 September 2004
AGD_USR.1	Xacta IA Manager Enterprise Edition Reference Manual – 24 September 2004
ATE_COV.1	Test Coverage Analysis for Xacta IA Manager Enterprise Edition Version 4.0 SP2 – 11 August 2004
ATE_FUN.1	Security Test Plan for Xacta IA Manager Enterprise Edition Version 4.0 SP2 – 26 September 2004 with Test Procedures
ATE_IND.2	Xacta IA Manager –Enterprise Edition V4.0 SP2 build 485
AVA_SOF.1	Strength of Function Analysis for Xacta IA Manager Enterprise Edition Version 4.0 SP2 – 11 August 2004
AVA_VLA.1	Vendor Vulnerability Analysis for Xacta IA Manager Enterprise Edition Version 4.0 SP2 – 07 October 2004

7 PP Claims

The Xacta IA Manager Enterprise Edition 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. Rationale is provided for each threat below the table.

Table 8-1 All Threats to Security Countered

Threat Name	Threat Description	Security Objective
T.Abuse	An undetected compromise of the TOE may occur as a result of an authorised user of the TOE (intentionally or otherwise) performing actions the individual is authorised to perform.	O.Access O.Attributes O.Audit O.IDAuth OE.Time
T.Access	An authorised 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.	O.Access O.Attributes O.Audit O.IDAuth OE.Time
T.BadPassword	Users may not select good passwords on their own, allowing attackers to guess their passwords and obtain unauthorised access to the TOE.	O.PasswordQual O.ProtectAuth
T.Bypass	An attacker may attempt to bypass TSF security functions.	O.NonBypass
T.Mismanage	Authorised administrators may make errors in the management of security functions and TSF data, if administrative tools are not provided. Administrative errors may allow attackers to gain unauthorised access to resources protected by the TOE.	O.Admin O.Roles
T.Privil	An unauthorised user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.	O.Access O.Attributes O.LoginNameQual O.IDAuth O.ProtectAuth
T.Tamper	An attacker may attempt to modify TSF programs and data.	OE.ProtectData
T.Transmit	TSF data may be disclosed or modified by an attacker while being transmitted between the TOE and its users.	OE.ProtectComm
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.	O.Audit OE.Time
T.Walkaway	A user may leave his workstation without logging out. A user may leave his workstation without logging out thus allowing unauthorized users to gain access to resources and data protected by the TOE.	O.Re-authenticate

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

- O.Access: The TOE must allow authorised users to access only appropriate TOE functions and data. This objective counters this threat by providing access controls that limit the actions an individual is authorised to perform.

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

T.Access: An authorised 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 must allow authorised users to access only appropriate TOE functions and data. This objective counters this threat by providing access controls that limit the actions an individual is authorised to perform.
- O.Attributes: The TOE must be able to store and maintain attributes. This objective counters this threat by requiring the TOE to store and maintain attributes. These attributes associate users with accounts and privileges that the Xacta IA Manager Enterprise Edition Access Control Policy is based on.
- O.Audit: The TOE must record audit records for data accesses and use of the TOE functions. This objective counters this threat by requiring the TOE to audit attempts for data accesses and use of TOE functions.
- O.IDAuth: The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data. This objective provides for authentication of users prior to any TOE data access.
- OE.Time: The IT environment must provide reliable time stamps. This objective provides for a reliable way to correlate audit records to reconstruct a potential compromise.

T.BadPassword: Users may not select good passwords on their own, allowing attackers to guess their passwords and obtain unauthorised access to the TOE. T.BadPassword is countered by:

- O.PasswordQual: The TOE must be able to specify password quality parameters such as password history, minimum length, and password compositions. This objective enables the administrator to specify checks for bad password qualities.
- O.ProtectAuth: The TOE will provide protected authentication feedback. When an authorised user account is typing in their password only asterisks will be seen on the screen. This will limit the ability to see what an authorised user account's password is.

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

- O.NonBypass: The TOE must ensure 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.

T.Mismanage: Authorised administrators may make errors in the management of security functions and TSF data, if administrative tools are not provided. Administrative errors may allow attackers to gain unauthorised access to resources protected by the TOE. T.Mismanage is countered by:

- O.Admin: The TOE must provide the functionality to enable authorised user(s) 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 must support multiple roles. Multiple roles can be used to enforce separation of duty, so that one administrator can catch errors made by another administrator.

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

- O.Access: The TOE must allow authorised users to access only appropriate TOE functions and data. This objective builds upon the O.IDAuth objective by only permitting authorised user accounts to access TOE functions.
- O.Attributes: The TOE must be able to store and maintain attributes. This objective counters this threat by requiring the TOE to store and maintain attributes. These attributes associate users with accounts and privileges that the Xacta IA Manager Enterprise Edition Access Control Policy is based on.
- O.LoginNameQual: The TOE must be able to specify login name minimum length requirements. This objective counters this threat by requiring the TOE to provide a minimum length qualifier for the user account name.
- O.IDAuth: The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data. This objective provides for authentication of user accounts prior to any TOE function access.
- O.ProtectAuth: The TOE will provide protected authentication feedback. When an authorised user is typing in their password only asterisks will be seen on the screen. This will limit the ability to see what an authorised user account holder's password is.

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

- OE.ProtectData: The IT Environment must protect passwords and project data. This objective counters this threat by preventing passwords from being modified by hashing stored passwords. In addition, backed up project data is encrypted.

T.Transmit: TSF data may be disclosed or modified by an attacker while being transmitted between the TOE and its users. T.Transmit is countered by:

- OE.ProtectComm: The IT environment must protect communications between the TOE and its users. This objective prevents data from being disclosed or modified when it is being transmitted between client and server components.

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 must record audit records for data accesses and use of the TOE functions. This objective records attempts to violate the security policy.
- OE.Time: The IT environment must provide reliable time stamps. This objective provides for a reliable way to correlate audit records to reconstruct a potential compromise.

T.Walkaway: A user may leave his workstation without logging out. A user may leave his workstation without logging out thus allowing unauthorized users to gain access to resources and data protected by the TOE. T.Walkaway is countered by:

- O.Re-authenticate: The TOE must be able to require the user to be re-authenticated after session time-out. Requiring re-authentication prevents an attacker from walking up to an unattended workstation and performing activities using the identity of the user account holder who left the workstation unattended.

8.1.2 Assumptions

Table 8-2 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 8-2 All Assumptions Addressed

Name	Assumption	Objective
A.Access	It is assumed that only authorized TOE, database, and operating system administrators have access to the data stored in the database and the underlying operating system.	ON.NoUntrusted
A.Admin	The administrator is trusted to correctly configure and operate the TOE according to the instructions provided by the TOE documentation.	ON.Install ON.Operations
A.Intranet	It is assumed that the Xacta IA Manager Enterprise Edition Server is deployed on a trusted intranet.	ON.Install
A.Manage	It is assumed that one or more authorised administrators are assigned who are competent to manage the TOE and the security of the information it contains, and who can be trusted not to deliberately abuse their privileges so as to undermine security.	ON.Person
A.NoUntrusted	It is assumed that there will be no untrusted users and no untrusted software on the Xacta IA Manager Enterprise Edition Server host.	ON.NoUntrusted
A.Physical	The TOE components critical to the security policy enforcement will be protected from unauthorized physical modification.	ON.Physical
A.Time	It is assumed that the underlying operating system provides reliable time stamps.	OE.Time
A.Users	It is assumed that users will protect their authentication data.	ON.ProtectAuth

A.Access: It is assumed that only authorized TOE, database, and operating system administrators have access to the data stored in the database and the underlying operating system. A.Access is covered by:

- ON.NoUntrusted: The administrator must ensure that there are no untrusted users and no untrusted software on the Xacta IA Manager Enterprise Edition Server host. This objective provides for the protection of the data store and operating system which the TOE relies on from the unauthorised access of untrusted software or users.

A.Admin: The 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 administrator on how to securely operate the TOE. This objective provides for operation procedures to be in place.

A.Intranet: It is assumed that the Xacta IA Manager Enterprise Edition Server is deployed on a trusted intranet. A.Intranet 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 XIAM-EE Server host on a trusted intranet. This objective provides for secure installation of the TOE.

A.Manage: It is assumed that one or more authorised administrators are assigned who are competent to manage the TOE and the security of the information it contains, and who can be trusted not to deliberately abuse their privileges so as to undermine security. A.Manage is covered by:

- ON.Person: Personnel working as authorised administrators shall be carefully selected and trained for proper operation of the system. This objective provides for competent personnel to administer the TOE.

A.NoUntrusted: It is assumed that there will be no untrusted users and no untrusted software on the Xacta IA Manager Enterprise Edition Server host. A.NoUntrusted is covered by:

- ON.NoUntrusted: The administrator must ensure that there are no untrusted users and no untrusted software on the Xacta IA Manager Enterprise Edition Server host. This objective provides for the protection of the TOE from untrusted software and users.

A.Physical: The TOE components critical to the security policy enforcement will be protected from unauthorized physical modification. 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 hardware and software.

A.Time: It is assumed that the underlying the operating system provides reliable time stamps. A.Time is covered by:

- OE.Time: The underlying operating system must provide reliable time stamps. This objective provides for reliable time stamps.

A.Users: It is assumed that users will protect their authentication data. A.Users is covered by:

- ON.ProtectAuth: The users must ensure that their authentication data is held securely and not disclosed to unauthorised persons. This objective provides for user account holders to protect their authentication data.

8.2 Security Requirements Rationale

8.2.1 Functional Requirements

Table 8-3 shows that all of the security objectives of the TOE are satisfied. Rationale for each objective is included below the table.

Table 8-3 All Objectives Met by Functional Components

Objective	Objective Description	Security Functional Requirement
O.Access	The TOE must allow authorised users to access only appropriate TOE functions and data.	FAU_SAR.2 Restricted audit review FDP_ACC.2 Complete access control FDP_ACF.1 Security attribute based access control FIA_AFL.1 Authentication failure handling FIA_UAU.2 User authentication before any action FIA_UID.2 User identification before any action FMT_MOF.1 Management of security functions behavior FMT_MTD.1 Management of TSF data FTA_TAB.1 Default TOE access banners
O.Admin	The TOE must provide the functionality to enable authorised user(s) to effectively manage the TOE and its security functions.	FAU_SAR.1 Audit review FAU_SAR.3 Selectable audit review FMT_MOF.1 Management of security functions behavior FMT_MSA.1 Management of security attributes FMT_MTD.1 Management of TSF data FMT_SMF.1 Specification of management functions
O.Attributes	The TOE must be able to store and maintain attributes.	FIA_ATD.1 User attribute definition
O.Audit	The TOE must record audit records for data accesses and use of the TOE functions.	FAU_GEN.1 Audit data generation FAU_GEN.2 User identity association FPT_STM.1 Reliable time stamps

Objective	Objective Description	Security Functional Requirement
O.IDAuth	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.	FIA_UAU.2 User authentication before any action FIA_UAU.6 Re-authenticating FIA_UID.2 User identification before any action
O.LoginNameQual	The TOE must be able to specify login name minimum length requirements.	FIA_SOS_EXP.1 Verification of login names
O.NonBypass	The TOE must ensure the security enforcing functions are invoked and succeed before allowing a TOE function to proceed.	FPT_RVM.1 Non-bypassability of the TSP
O.PasswordQual	The TOE must be able to specify password quality parameters such as password history, minimum length, and password compositions.	FIA_SOS.1 Verification of secrets
O.ProtectAuth	The TOE will provide protected authentication feedback.	FIA_UAU.7 Protected authentication feedback
O.Re-authenticate	The TOE must be able to require the user to be re-authenticated after session time-out.	FIA_UAU.6 Re-authenticating
O.Roles	The TOE must support multiple roles.	FMT_SMR.1 Security roles

O.Access: The TOE must allow authorised users to access only appropriate 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 authorised 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_AFL.1 Authentication failure handling, which requires the TSF to detect when an administrator configured maximum number of unsuccessful authentication attempts occur related to administrator, executive, and user login attempts. When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF will disable the administrator, executive, and user accounts until the account is reactivated by an authorised account holder.
- FIA_UAU.2 User authentication before any action, which requires each user account to be successfully authenticated before allowing access to the TOE.
- FIA_UID.2 User identification before any action, which requires that user account holders be successfully identified before allowing access to the TOE.
- FMT_MOF.1 Management of security functions behavior, which restricts the ability to disable, enable, and modify functions to authorised user account holders.
- FMT_MTD.1 Management of TSF data, which specifies the management of TSF Data according to assigned roles.
- FTA_TAB.1 Default TOE access banners, which requires that before establishing a user session, the TSF shall display an advisory warning message regarding unauthorised use of the TOE.

O.Admin: The TOE must provide the functionality to enable authorised user(s) to effectively manage the TOE and its security functions. O.Admin is addressed by:

- FAU_SAR.1 Audit review, which requires that the authorised administrator be able to read all audit records within the administrator's scope of control.
- FAU_SAR.3 Selectable audit review, which requires that the TSF will provide the ability to search, sort, and order audit data.
- FMT_MOF.1 Management of security functions behaviour, which requires that the built-in master administrator be able to manage the behavior of the audit tools.
- FMT_MSA.1 Management of security attributes, which enforces the Table 5-5 Management of Security Attributes to restrict the ability to create, query, modify, and delete the specified security attributes to the authorised account types.
- FMT_MSA.3 Static attribute initialisation, which requires the TSF enforce access control for 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.Attributes: The TOE must be able to store and maintain attributes. O.Attributes is addressed by:

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

O.Audit: The TOE must record audit records for data accesses and use of the TOE 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 account.
- FPT_STM.1 Reliable time stamps, which requires that a reliable time stamp be available to record in the audit record.

O.IDAuth: The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data. O.IDAuth is addressed by:

- FIA_UAU.2 User authentication before any action, which requires each user account to be successfully authenticated before allowing access to the TOE.
- FIA_UAU.6 Re-authenticating, which requires that the TSF re-authenticate the user account under the specified conditions.
- FIA_UID.2 User identification before any action, which requires that user account holders be successfully identified before allowing access to the TOE.

O.LoginNameQual: The TOE must be able to specify login name minimum length requirements. O.LoginNameQual is addressed by:

- FIA_SOS_EXP.1 Verification of login names, which requires the TSF provide a mechanism to verify that the login name meets the minimum number of characters required in all login names.

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

- FPT_RVM.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.PasswordQual: The TOE must be able to specify password quality parameters such as password history, minimum length, and password compositions. O.PasswordQual is addressed by:

- FIA_SOS.1 Verification of secrets, which requires that the TSF provide a mechanism to verify that passwords meet the rules of the password policy.
- FIA_SOS_EXP.1 Verification of login names, which requires that the TSF provide a mechanism to verify that the login name meets the minimum number of characters required in all login names.

O.ProtectAuth: The TOE will provide protected authentication feedback. O.ProtectAuth is addressed by:

- FIA_UAU.7 Protected authentication feedback, the TSF shall provide only a display of the typed in user account name and asterisks for the password for password authentication.

O.Re-authenticate: The TOE must be able to require the user account to be re-authenticated. O.Re-authenticate is addressed by:

- FIA_UAU.6 Re-authenticating, which requires that the TSF re-authenticate the user account under the specified conditions.

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

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

8.2.2 Dependencies

Table 8-4 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. If the TOE dependency is met by an SFR in the IT environment an "E" will be next to the reference number.

Table 8-4 TOE Dependencies Satisfied

No.	Component	Component Name	Dependencies	Reference
1.	FAU_GEN.1	Audit data generation	FPT_STM.1	29 E
2.	FAU_GEN.2	User identity association	FAU_GEN.1	1
			FIA_UID.1	15 (H)
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.	FDP_ACC.2	Complete access control	FDP_ACF.1	8
7.	FDP_ACF.1	Security attribute based access control	FDP_ACC.1	7 (H)
			FMT_MSA.3	18
8.	FIA_AFL.1	Authentication failure handling	FIA_UAU.1	12 (H)
9.	FIA_ATD.1	User attribute definition	None	None
10.	FIA_SOS.1	Verification of secrets	None	None
11.	FIA_SOS_EXP.1	Verification of login names	None	None
12.	FIA_UAU.2	User authentication before any action	FIA_UID.1	15 (H)
13.	FIA_UAU.6	Re-authenticating	None	None
14.	FIA_UAU.7	Protected authentication feedback	FIA_UAU.1	12 (H)
15.	FIA_UID.2	User identification before any action	None	None
16.	FMT_MOF.1	Management of security functions behavior	FMT_SMR.1	21
			FMT_SMF.1	20
17.	FMT_MSA.1	Management of security attributes	FDP_ACC.1	7 (H)
			FMT_SMR.1	21
			FMT_SMF.1	20

No.	Component	Component Name	Dependencies	Reference
18.	FMT_MSA.3	Static attribute initialisation	FMT_MSA.1	17
			FMT_SMR.1	21
19.	FMT_MTD.1	Management of TSF data	FMT_SMR.1	21
			FMT_SMF.1	20
20.	FMT_SMF.1	Specification of management functions	None	None
21.	FMT_SMR.1	Security roles	FIA_UID.1	15 (H)
22.	FPT_RVM.1	Non-bypassability of the TSP	None	None
23.	FTA_TAB.1	Default TOE access banners	None	None

Table 8-5 IT Environment Dependencies are Satisfied

No.	Component	Component Name	Dependencies	Reference
24.	FCS_CKM.1	Cryptographic key generation	FCS_COP.1	26 E
			FCS_CKM.4	25 E
			FMT_MSA.2	28 E
25.	FCS_CKM.4	Cryptographic key destruction	FCS_CKM.1	24 E
			FMT_MSA.2	28 E
26.	FCS_COP.1*	Cryptographic operation	FCS_CKM.1	24 E
			FCS_CKM.4	25 E
			FMT_MSA.2	28 E
27.	FMT_MSA.2	Secure security attributes	ADV_SPM.1	See section 8.2.3
			FDP_ACC.1	7 (H)
			FMT_MSA.1	17
			FMT_SMR.1	21
28.	FPT_STM.1	Reliable time stamps	None	None
29.	FTP_TRP.1	Trusted Path	None	None

8.2.3 Rationale why dependencies are not met

For FMT_MSA.2, ADV_SPM.1 is not included because ADV_SPM.1 requires the TOE developer to provide an informal TOE security policy (TSP) model. The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled. It is the objective of the ADV_SPM family to provide additional assurance that the security functions in the functional specification enforce the policies in the TSP. This is accomplished via the development of a security policy model that is based on a subset of the policies of the TSP, and establishing a correspondence between the functional specification, the security policy model, and these policies of the TSP. Since the cryptographic functions are provided by the environment and not by the TOE, the functional specification will not include the cryptographic functions. As a result, there is no way to map the functional specification to the security policy model.

8.2.4 Strength of Function Rationale

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. As stated in section 6.1.4, there are some security functions based on probabilistic methods. See section 5.2.7 for the objectives that SOF supports. The specific “strength” required of the methods used to provide difficult-to-guess passwords are defined in Table 5-4 Password Policy Rules. These map to the Security Functions: MUA-4 and MUA-5. MUA-5 requires a minimum length for user account names.

8.2.5 Assurance Rationale

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

8.2.6 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 builds on the others. 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 TSF shall provide the built-in master administrator and site-level administrator with the capability to read all audit information from the audit records. In addition, FAU_SAR.1 gives the folder-level administrator access to read all audit records that are within the folder-level administrator's scope of control. 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 authorised administrator the ability to perform searches, sorting, and ordering of the audit event data. Audit records are generated for many events where other requirements are coming to bear, such as login, policy check failures, and management functions.

Together FDP_ACC.2 and FDP_ACF.1 provide User Data Protection. FDP_ACC.2 defines the Xacta IA Manager Enterprise Edition Access Control Policy. FDP_ACF.1 specifies that the TSF enforces access based upon security attributes. The subjects with roles of the following listed in Table 5-3 (FDP_ACC.2) are also defined in FMT_SMR.1.

Login processing brings in elements of many requirements, but all in a complementary way. The login starts with an invocation of the trusted path mechanism (see FTP_TRP.1). FIA_UID.2 wants the user identified before allowing any other operations and FIA_UAU.2 wants the user authenticated before allowing any other operations. FIA_SOS.1 defines the strength of the authentication. FIA_SOS_EXP.1 defines the minimum required characters for a user name. FIA_UAU.7 requires that feedback from authentication input be obscured. FIA_ATD.1 specifies the security attributes belonging to individual users. FIA_UAU.6 specifies that users must re-authenticate after a configurable session time-out. FIA_AFL.1 specifies authentication failure handling to control the number of failed access attempts.

The management requirements (FMT_) are related to many of the other requirements. FMT_MOF.1 provides for the management of the audit functions (FAU_GEN.1). FMT_MSA.1 enforces the Xacta IA Manager Enterprise Edition Access Control Policy (FDP_ACC.2). FMT_MSA.3 enforces the Xacta IA Manager Enterprise Edition Access Control Policy to provide restrictive default values for security attributes. FMT_MTD.1 specifies the management of TSF Data according to assigned roles. FMT_SMF.1 which specifies the security management functions of the TSF. In many cases, the other functions will enforce the settings made through the management functions. Installation functions (see ADO_IGS.1) rely on management functions. The administrator guidance (see AGD_ADM) documents the management functions. Use of many of the management functions relies on the use of the trusted path mechanism (FTP_TRP.1).

FPT_RVM.1 makes certain the Xacta IA Manager Enterprise Edition Access Control Policy (FDP_ACC.2) is invoked and succeeds before any other functions within the TOE's Scope of Control are allowed to proceed.

8.2.7 Requirements for the IT Environment

Table 8-6 shows that all of the security objectives for the IT environment are satisfied. Rationale for each objective is included below the table.

Table 8-6 All Objectives for the IT Environment map to Requirements in the IT environment

Objective	Objective Description	Requirement for the IT Environment	Component Title
OE.ProtectComm	The IT environment must protect communications between the TOE and its users.	FTP_TRP.1	Trusted path
OE.ProtectData	The IT Environment must protect passwords and project data.	FCS_CKM.1	Cryptographic key generation
		FCS_CKM.4	Cryptographic key destruction
		FCS_COP.1*	Cryptographic operation
OE.Time	The underlying operating system must provide reliable time stamps.	FPT_STM.1	Reliable time stamps

OE.ProtectComm: The IT environment must protect communications between the TOE and its users. OE.ProtectComm is addressed by:

- FCS_CKM.1 Cryptographic key generation, which requires the IT environment generate cryptographic keys in accordance with a specified cryptographic key generation algorithm and specified cryptographic key sizes that meet a specified standard.
- FCS_CKM.4 Cryptographic key destruction, which requires the IT environment, shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method.
- FCS_COP.1-1 Cryptographic operation, which requires that the IT environment perform cryptographic operations in accordance with a specified cryptographic algorithm and cryptographic key sizes that meet a specified standard.
- FTP_TRP.1 Trusted path, which requires the IT environment provides a communication path between the TSF and remote and local users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.

OE.ProtectData: The IT Environment must protect passwords and project data. OE.ProtectData is addressed by:

- FCS_CKM.1 Cryptographic key generation, which requires the IT environment generate cryptographic keys in accordance with a specified cryptographic key generation algorithm and specified cryptographic key sizes that meet a specified standard.
- FCS_CKM.4 Cryptographic key destruction, which requires the IT environment, shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method.
- FCS_COP.1-1 Cryptographic operation, which requires that the IT environment perform cryptographic operations in accordance with a specified cryptographic algorithm and cryptographic key sizes that meet a specified standard.

- FCS_COP.1-2 Cryptographic operation, which requires that the IT environment perform hashing operations in accordance with a specified cryptographic algorithm and cryptographic key sizes that meet a specified standard.

OE.Time The underlying operating system must provide reliable time stamps. OE.Time is addressed by:

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

8.3 TOE Summary Specification Rationale

8.3.1 IT Security Functions

Table 8-7 shows that the IT Security Functions in the TOE Summary Specification (TSS) address all of the TOE Security Functional Requirements.

Table 8-7 Mapping of Functional Requirements to TOE Summary Specification

Item	Functional Component	Functional Requirement	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.
			SA-2	Specifies the information to be recorded in an audit record.
2.	FAU_GEN.2	User identity association	SA-3	Each auditable event is associated with the identity of the user account that caused the event.
3.	FAU_SAR.1	Audit review	SA-4	Specifies who has the capability to read information from the audit records.
4.	FAU_SAR.2	Restricted audit review	SA-5	Specifies that only specific user accounts have read access to the audit records.
5.	FAU_SAR.3	Selectable audit review	SA-6	Specifies that Xacta IA Manager Enterprise Edition provides the ability to perform searches, sorting, and ordering of the audit data, based on various criteria.
6.	FDP_ACC.2	Complete access control	MUA-1	Specifies the Xacta IA Manager Enterprise Edition Access Control Policy.
7.	FDP_ACF.1	Security attribute based access control	MUA-1	Specifies the subjects and objects controlled under the Xacta IA Manager Enterprise Edition Access Control Policy.
8.	FIA_AFL.1	Identification and authentication	MUA-2	Specifies that Xacta IA Manager Enterprise Edition detects when an administrator configured maximum number of unsuccessful authentication attempts occur related to administrator, executive, and user account login attempts. When the defined number of unsuccessful authentication attempts has been met or surpassed, Xacta IA Manager Enterprise Edition disables the administrator, executive, and user accounts until the account is reactivated by an authorised account holder.

Item	Functional Component	Functional Requirement	Requirement is met by:	
			Security Function Ref. No	Rationale
9.	FIA_ATD.1	User attribute definition	MUA-3	Specifies the security attributes maintained for each user account.
10.	FIA_SOS.1	Verification of secrets	MUA-4	Specifies that user account passwords meet the rules of the password policy.
11.	FIA_SOS_EXP.1	Verification of login names	MUA-5	Specifies that user account login names meet a minimum number of characters.
12.	FIA_UAU.2	User authentication before any action	UL-1	Specifies that the Xacta IA Manager Enterprise Edition requires each user account to successfully authenticate with a password before being allowed any other actions.
13.	FIA_UAU.6	Re-authenticating	UL-2	Specifies the Xacta IA Manager Enterprise Edition requires the user account to re-authenticate under certain conditions.
14.	FIA_UAU.7	Protected authentication feedback	UL-3	Specifies that the Xacta IA Manager Enterprise Edition displays only the typed in user account name and asterisks for the password during password authentication.
15.	FIA_UID.2	User identification before any action	UL-4	Specifies the Xacta IA Manager Enterprise Edition requires each user to identify himself/herself before being allowed to perform any other actions.
16.	FMT_MOF.1	Management of security functions behavior	SM-1	Specifies that Xacta IA Manager Enterprise Edition restricts the ability to determine the behavior of, disable, enable, and modify the behavior of the functions related to the audit function (see FAU_GEN.1.1) to the Built-in Master Administrator.
17.	FMT_MSA.1	Management of security attributes	SM-2	Specifies that Xacta IA Manager Enterprise Edition restricts the ability to query, modify, delete, or create the specified security attributes see Table 5-5 to the specified user accounts see Table 5-5.
18.	FMT_MSA.3	Static attribute initialisation	SM-3	Specifies that Xacta IA Manager Enterprise Edition provides restrictive default values for security attributes and the Built-in Master Administrator, Site-Level administrator, and Folder-Level administrator can specify alternative initial values.
19.	FMT_MTD.1	Management of TSF data	SM-4	Specifies that Xacta IA Manager Enterprise Edition restricts the ability to access data.
20.	FMT_SMF.1	Specification of management functions	SM-5	Specifies the security management functions provided by Xacta IA Manager Enterprise Edition.
21.	FMT_SMR.1	Security roles	SM-6	Specifies the roles maintained in the Xacta IA Manager Enterprise Edition.

Item	Functional Component	Functional Requirement	Requirement is met by:	
			Security Function Ref. No	Rationale
22.	FPT_RVM.1	Non-bypassability of the TSP	MUA-6	Specifies Xacta IA Manager Enterprise Edition ensures that the Table 5-3 Xacta IA Manager Enterprise Edition Access Control Policy is invoked and succeeds before each function is allowed to proceed.
23.	FTA_TAB.1	Default TOE access banners	UL-5	Specifies Xacta IA Manager Enterprise Edition displays an advisory warning message regarding unauthorised use of the TOE.

8.3.2 Assurance Measures

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

Table 8-8 Assurance Measures Rationale

Component	Evidence Requirements	How Satisfied	Rationale
ACM_CAP.2	CM Documentation • CM Proof • Configuration Item List	Configuration Items for Xacta IA Manager Enterprise Edition Version 4.0 SP2 – 01 December 2004 • Xacta_ACM_SP2_041201 FINAL.doc • SP2_Detect_Modules FINAL.doc • SP2_Publisher_Modules FINAL.doc • SP2_XIAM_Modules Query_AppServer FINAL.doc • SP2_XIAM_Modules Query_GUI FINAL.doc	• 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
ADO_DEL.1	Delivery Procedures	Delivery Procedures for Xacta IA Manager Enterprise Edition Version 4.0 SP2 – 26 September 2004 Xacta_DEL_SP2_040926 FINAL.doc	Provides a description of all procedures that are necessary to maintain security when distributing Xacta IA Manager Enterprise Edition software to the user's site. - Applicable across all phases of delivery from packaging, storage, distribution

Component	Evidence Requirements	How Satisfied	Rationale
ADO_IGS.1	Installation, generation, and start-up procedures	Secure Installation & Configuration Supplement for for Xacta IA Manager Enterprise Edition Version 4.0 SP2 – 03 November 2004 Xacta_IGS_SP2_041103 FINAL.doc	Provides detailed instructions on how to install Xacta IA Manager Enterprise Edition.
ADV_FSP.1	Functional Specification	Security Functional Specification for Xacta IA Manager Enterprise Edition Version 4.0 SP2 – 09 November 2004 Xacta_FSP_SP2_041109 FINAL.doc	Provides rationale that TSF is fully represented
		Xacta IA Manager Enterprise Edition Reference Manual – 24 September 2004 Assessment Engine Manual 040924 FINAL.pdf	Describes the TSF interfaces and TOE functionality
ADV_HLD.1	High-Level Design	High Level Design for Xacta IA Manager Enterprise Edition Version 4.0 SP2 – 21 August 2004 Xacta_HLD_SP2_040821 FINAL.doc Xacta_HLD_AppxA_SP2_040821 FINAL.doc Xacta_HLD_AppxB_SP2_040821 FINAL.doc	Describes the TOE subsystems and their associated security functionality
		Xacta IA Manager Enterprise Edition Reference Manual – 24 September 2004 Assessment Engine Manual 040924 FINAL.pdf	
ADV_RCR.1	Representation Correspondence	Informal Correspondence Demonstration for Xacta IA Manager Enterprise Edition Version 4.0 SP2 – 21 August 2004 Xacta_RCR_SP2_040821 FINAL.doc	Provides the following two dimensional mappings: 1. TSS and functional specification; 2. Functional specification and high-level design.
AGD_ADM.1	Administrator Guidance	Xacta IA Manager Enterprise Edition Reference Manual – 24 September 2004 Assessment Engine Manual 040924 FINAL.pdf	Describes how to administer the TOE securely.

Component	Evidence Requirements	How Satisfied	Rationale
AGD_USR.1	User Guidance	Xacta IA Manager Enterprise Edition Reference Manual – 24 September 2004 Assessment Engine Manual 040924 FINAL.pdf	Describes the secure use of the TOE.
ATE_COV.1	Test Coverage Analysis	Test Coverage Analysis for Xacta IA Manager Enterprise Edition Version 4.0 SP2 – 11 August 2004 Xacta_COV_SP2_040811 FINAL.doc	Shows correspondence between the tests identified in the test documentation and the TSF as described in thefunctional specification.
ATE_FUN.1	Test Documentation	Security Test Plan for Xacta IA Manager Enterprise Edition Version 4.0 SP2 – 26 September 2004 Xacta_FUN_TestPlan_SP2_040926 FINAL.doc Build 485 Test Cases.zip	Test documentation includes test plans and procedures and expected and actual results.
ATE_IND.2	TOE for Testing	Xacta IA Manager –Enterprise Edition V4.0 SP2 build 485	The TOE will be provided for testing.
AVA_SOF.1	SOF Analysis	Strength of Function Analysis for Xacta IA Manager Enterprise Edition Version 4.0 SP2 – 11 August 2004 Xacta_SOF_SP2_040811 FINAL.doc	Provides a rationale that each mechanism identified in the ST as having an SOF meets or exceeds the minimum strength level specified there.
AVA_VLA.1	Vulnerability Analysis	Vendor Vulnerability Analysis for Xacta IA Manager Enterprise Edition Version 4.0 SP2 – 07 October 2004 Xacta_VLA_SP2_041007 FINAL.doc	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.

8.5 Explicitly Stated Requirements Rationale

FIA_SOS_EXP.1 had to be explicitly stated because there is not an existing SFR in the CC Part 2 that describes a mechanism to verify that the login name meet the minimum number of characters required in all login names. A refinement adds additional detail and narrows the scope. A refinement of the FIA_SOS.1 would not correctly describe the functionality of the TSF providing a mechanism to verify that the login name meet the minimum number of characters required in all login names.

9 Acronyms

C&A	Certification and Accreditation
CC	Common Criteria [for IT Security Evaluation]
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
ID	Identifier
IT	Information Technology
SF	Security Function
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TOE Security Functions Interface
TSP	TOE Security Policy

10 References

CCITSE	*Common Criteria for Information Technology Security Evaluation*, CCIMB-2004-01-002, Version 2.2, January 2004.
Application_Reference_Manual.pdf	Xacta IA Manager Assessment Engine Reference Manual