National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Xacta® IA Manager: Assessment Engine and Xacta® IA Manager: Continuous Assessment, Version 4.0 Service Pack 8 (Commercial and Government Distribution Packages)

Report Number: CCEVS-VR-VID10318
Dated: September 16, 2010
Version: 1.0

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

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

ACKNOWLEDGEMENTS

Validation Team

Mr. Daniel Faigin

The Aerospace Corporation

El Segundo, California

(Lead Validator)

Mr. Jerome Myers

The Aerospace Corporation

Columbia, Maryland

(Senior Validator)

Common Criteria Testing Laboratory (CCTL)

Mr. Herbert Markle

CygnaCom Solutions

McLean, Virginia

Much of the material in this report was extracted from evaluation material prepared by the CCTL. The CCTL team deserves credit for their hard work in developing that material. Many of the product descriptions in this report were extracted from the Security Target for Xacta® IA Manager: Assessment Engine and Xacta® IA Manager: Continuous Assessment, Version 4.0 Service Pack 8 (Commercial and Government Distribution Packages)

Table of Contents

List of Figures

1. Executive Summary

This Validation Report (VR) documents the evaluation and validation of the product Xacta® IA Manager: Assessment Engine and Xacta® IA Manager: Continuous Assessment, Version 4.0 Service Pack 8 (Commercial and Government Distribution Packages). The TOE can be purchased as either a commercial or government package. The government package contains the TOE along with a folder of government standard templates. The commercial package contains the TOE and a folder of commercial templates.

The TOE is the same in both the commercial and government package. The entire TOE will be referred to as Xacta IA Manager.

This VR is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

Xacta IA Manager is a continuous risk management framework that manages and supports IT security risk and compliance assessment activities for an organization. The TOE includes project templates, which are based on known assessment methods such as DCID, DIACAP, DITSCAP, NIST, COBIT, or ISO 27001, and that contain workflow tasks and process steps to perform a certification assessment. The TOE provides the mechanisms to help customers through the steps of collecting data from an enterprise's assets (which may include physical security, organizational procedures and processes, personnel, physical IT assets, etc.), evaluating risk and compliance to a requirement, and publishing pre-formatted document(s) that would then be submitted to the appropriate DAA (Designated Approving Authority) or AO (Authorizing Official).

Note: The correctness and conformance of the templates to any government or commercial standard is by Vendor assertion. Verifying the correctness and conformance of the templates to any standard, the correctness of the assessment scripts for the assessment task, or that the process steps defined by the templates are complete and sufficient was not part of this evaluation.

The main TOE components are the Assessment Engine component and the Continuous Assessment component, which is made up of the Asset Manager and Detect Server subsystems and the HostInfo Agents. Each of the Assessment Engine (AE), Asset Manager (AM), and Detect Server (DS) components has a web interface for its operational functions. HostInfo Agents collect information about the network asset it resides on via assessment scripts. The scripts are cryptographically signed and assigned (tasked) at the Asset Manager. The Asset Manger then transmits the task to the Detect Server, which is responsible to transfer the signed scripts to the HostInfo Agents. The HostInfo Agent then executes the signed scripts and securely transmits the results to the Detect Server. The Detect Server then syncs this information with the Asset Manger. The Assessment Engine uses the continuously updated information from the Asset Manger to conduct the risk and compliance assessments.

The TOE provides the following security functionality: auditing of security relevant events, TOE user account administration, ability to add a signature to published reports and assessment scripts as proof of origin, TOE user identification and authentication,

security role based access to management functions, trusted channel communication between components, and risk and compliance assessment support functions.

The TOE uses cryptographic functions for trusted communications and digital signatures. In particular, cryptographic functionality is provided for:

- Local Password Storage*
- PKI Authentication
- OCSP Revocation Checking
- External Authentication Server Data Storage*
- 3rd Party Application Password Storage*
- Data transmitted between AE and Publisher*
- Communications between TOE Components*
- Communications between TOE and External Servers*
- Communications between TOE and Xacta Customer Support Server*
- Communications between TOE and Network Assets*
- Project Backup and Restore*
- Digital Signatures for Test Scripts
- Digital Signatures for Documents and Reports

*Note: Not all cryptographic functions used by the TOE have been FIPS certified. The correctness of these cryptographic modules used by the TOE is by Vendor assertion; the correctness and conformance of these modules to any standard was not part of this evaluation. Those functions marked with an * use the FIPS certified RSA BSafe Crypto-J v3.6 JSafe Software Module (cert #812) or JCE Provider Module (cert #820). For the other functions, the cryptography has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation.*

The TOE is intended for use:

- In a system high environment where all data is controlled to the highest level of security classification assigned to the operating environment.
- In computing environments where there is a low level threat of malicious attacks. The assumed level of expertise of the attacker for all the threats is unsophisticated.

CC Compliance requires the TOE to be configured according to the instructions in the document: *Secure Installation & Configuration Supplement For Xacta® IA Manager: Assessment Engine and Xacta® IA Manager: Continuous Assessment, Version 4.0 Service Pack 8 (Commercial and Government Distribution Packages),* Version 4.1, 23 July 2010.

The evaluation was performed by the CygnaCom Common Criteria Testing Laboratory (CCTL), and was completed in August 2010. The information in this report is derived

from the Evaluation Technical Report (ETR) and associated test reports, all written by the CygnaCom CCTL. The evaluation team determined that the product is Common Criteria version 3.1 R2 [CC] Part 2 extended and Part 3 conformant, and meets the assurance requirements of EAL 2 augmented with ALC_FLR.2 from the Common Methodology for Information Technology Security Evaluation, Version 3.1 R2, [CEM]. This Security Target does not claim conformance to any U.S. Government Protection Profile.

The evaluation and validation were consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site www.niap-ccevs.org. The Security Target (ST) is contained within the document Security Target for Xacta® IA Manager: Assessment Engine and Xacta® IA Manager: Continuous Assessment, Version 4.0 Service Pack 8 (Commercial and Government Distribution Packages)

2. Identification

Target of Evaluation:

Xacta® IA Manager: Assessment Engine and Xacta® IA Manager: Continuous Assessment, Version 4.0 Service Pack 8 (Commercial and Government Distribution Packages)

Evaluated Software:

Xacta® IA Manager: Assessment Engine and Xacta® IA Manager: Continuous Assessment, Version 4.0 Service Pack 8 (Commercial and Government Distribution Packages)

Assessment Engine Build 22212

Asset Manager Build 4974

Detect Server Build 3249

HostInfo – Windows (32 bit) Build 1875

HostInfo – Windows (64 bit) Build 1875

HostInfo – Mac Build 1793

HostInfo – Unix (Solaris and Red Hat) Build 1878

Developer:	Telos Corporation
CCTL:	CygnaCom Solutions 7925 Jones Branch Dr, Suite 5200 McLean, VA 22102-3321
Evaluators:	Herb Markle
Validation Scheme:	National Information Assurance Partnership Common Criteria Evaluation and Validation Scheme (CCEVS)
Validators:	Daniel Faigin, Jerome Myers.
CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 3.1 R2, September 2007
CEM Identification:	Common Methodology for Information Technology Security Evaluation, Version 3.1 R2, September 2007

3. Security Policy

The TOE's security policy is expressed in the security functional requirements identified in the section 6.1 in the ST. Potential users of this product should confirm that functionality implemented is suitable to meet the user's requirements.

The TOE provides the following security features:

3.1. Security Audit

The TOE provides a de-centralized auditing functionality. The TOE provides its own auditing capabilities separate from those of the host operating systems. The TOE provides the ability to search, sort, order, and view its own audit records.

Security Audit relies on functionality in the Operational Environment to provide: protection of the audit information stored in the TOE components' databases and in files on the TOE platforms' operating system; access to the audit information stored in an external or local Syslog; the ability to view and configure the HostInfo Agent logs; and reliable timestamps for the audit records.

3.2. Proof of Origin

The TOE provides the ability for administrators to digitally sign documents, reports and scripts to verify the origin of the information contained within them.

Proof of Origin relies on functionality in the Operational Environment to provide: PKI Infrastructure functionality; Adobe Acrobat digital signing functionality; and use of an optional Browser Crypto Module or CAC as a security provider for generation of digital signatures.

Note: The cryptographic functions used for digitally signing documents and scripts have not been FIPS certified. The correctness of these cryptographic modules used by the TOE is by Vendor assertion; the correctness and conformance of these modules to any standard was not part of this evaluation.

3.3. Identification and Authentication

The TOE provides user identification and authentication for access to the administrative interfaces (the Dashboard, Asset Manager GUI, and Detect Server GUI) and access to TSF data through the use of user accounts. Each account holder must be successfully identified and authenticated with a username and password by the TSF or by an authentication service invoked by the TSF before access to the TOE is allowed. In addition the TSF enforces a password policy and requires users to be re-authenticated after a specified period of inactivity.

The TOE enhances the security of an individual's TOE session by displaying a warning message (banner) when the session is initiated. The individual must re-authenticate if a session is terminated because of an inactivity time-out.

Identification and Authentication relies on functionality in the Operational Environment (OE) to provide: PKI Infrastructure functionality including keystore; protection of the

user account information stored in the TOE components' databases; encryption support; use of an optional external authentication server; and trusted communications between the TOE and any external authentication server.

Note: The cryptographic functions used for certificate authentication and revocation checking have not been FIPS certified. The correctness of these cryptographic modules used by the TOE is by Vendor assertion; the correctness and conformance of these modules to any standard was not part of this evaluation.

3.4. Security Management

The TOE provides security management through the use of administrator interfaces. Through the enforcement of an administrative access control policy, access to the management functionality and TSF data is controlled by security (administrative) role assignments.

Security Management relies on functionality in the Operational Environment to provide: protection of the HostInfo Agent Configuration Utility; and trusted communications between the TOE and external servers.

3.5. Trusted Channel

The TOE provides for trusted communication channels among its distributed application components by invoking the secure communications functionality of the Operational Environment and by providing cryptographic functions using third-party algorithms.

Trusted Channel relies on functionality in the Operational Environment for TCP/IP protocols.

Note: *The cryptographic functions used for secure communications between TOE components have been FIPS certified (RSA BSafe Crypto-J v3.6 JSafe Software Module (cert #812) and JCE Provider Module (cert #820)). The correctness of cryptographic modules used by the TOE for other purposes is by Vendor assertion; the correctness and conformance of those modules to any standard was not part of this evaluation.*

3.6. Risk and Compliance Assessment

The TOE provides risk and compliance assessment of IT network assets including: collection of asset data, evaluation of the collected data, and sending notifications to appropriate personnel for significant events in the assessment process.

Note: The correctness and conformance of the templates to any government or commercial standard is by Vendor assertion. Verifying the correctness and conformance of the templates to any standard, the correctness of the assessment scripts for the assessment task, or that the process steps defined by the templates are complete and sufficient was not part of this evaluation.

Risk and Compliance Assessment relies on functionality in the Operational Environment to provide: proper configuration of the HostInfo Agent platforms for proper data collection; optional third-party asset discovery/vulnerability scanning; optional third-party enterprise management database functionality; PKI Infrastructure functionality;

protection of data and script files on the host platforms; trusted communications between the TOE and the host platforms; and optional SMTP Server functionality for Asset Notification.

3.7. Summary

3.7.1. Security Functional Requirements

A list of the SFRs for the TOE follows

Note that _EXT in the SFR ID indicates extended requirements. The ST must be consulted for the specifics of the _EXT requirements and the completions of the SFRs drawn from the CC.

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. FCO_SIG_EXT.1-1: Generation of digital signatures (documents and reports)
7. FCO_SIG_EXT.1-2: Generation of digital signatures (scripts)
8. FCS_CKM.1: Cryptographic key generation
9. FCS_CKM.4: Cryptographic key destruction
10. FCS_COP.1: Cryptographic operation
11. FIA_AFL.1: Authentication failure handling
12. FIA_ATD.1: User attribute definition
13. FIA_SOS.1: Verification of secrets
14. FIA_UAU_EXT.2: TSF user authentication before any action
15. FIA_UAU.6: Re-authenticating
16. FIA_UAU.7: Protected authentication feedback
17. FIA_UID.2: User identification before any action
18. FMT_MTD.1: Management of TSF data
19. FMT_SMF.1: Specification of Management Functions
20. FMT_SMR.1: Security roles
21. FTA_SSL_EXT.1: TSF-initiated session locking
22. FTA_TAB.1: Default TOE access banners
23. FTP_ITC_EXT.1 : Partial Intra-TSF trusted channel among distributed TOE components

24. RCA_COL_EXT.1: Asset data collection
25. RCA_EVL_EXT.1: Risk and compliance evaluation
26. RCA_NOT_EXT.1: Asset security notifications

3.7.2. Operational Environment Objectives

The TOE's operating environment must satisfy the following objectives.

1. The Operational Environment will provide an authentication service for user identification and authentication that can be invoked by the TSF to control a user's logical access to the TOE.

   Note: This objective is only applicable to the TOE is configured to use an external authentication service. (I.e. LDAP or Active Directory Server)
2. The administrator will ensure that there are no untrusted users and no untrusted software on the TOE component servers.
3. The TOE will be installed, configured and operated in a secure manner as outlined in the supplied guidance.
4. Personnel working as authorized administrators will be carefully selected and trained for proper operation of the system.
5. Those responsible for the TOE will ensure that those parts of the TOE critical to the security policy are protected from any physical attack.
6. The Operational Environment will provide a means for secure storage and protection of the TOE audit information from unauthorized users via the Operational Environment interfaces.
7. Users will ensure that their authentication data is held securely and not disclosed to unauthorized persons.
8. Those responsible for the TOE will ensure the communications between the TOE components and between the TOE components and remote users are via a secure channel.
9. The Operational Environment will be configured by those responsible for the TOE to protect information stored in the database systems used by the TOE via the Operational Environment interfaces.
10. The Operational Environment will be configured by those responsible for the TOE to protect executable and data files used by the TOE via the Operational Environment interfaces.
11. The Operational Environment will provide mechanisms to support digital signing of files to prove the origin of the information contained within them.
12. The Operational Environment will provide a mechanism to establish a trusted communications path that provides for the protection of the data from modification or disclosure while being exchanged between TOE components and agents.

13. The underlying operating system will provide reliable time stamps.
14. Responsible personnel will configure each host computer on which the HostInfo Agent has been installed to allow the agent to collect the data the TOE needs for risk and compliance assessment.

4. Assumptions and Clarification of Scope

4.1. Usage Assumptions

For secure usage, the operational environment must be managed in accordance with the documentation associated with the following EAL 2 assurance requirements.

a) AGD_OPE.1 Operational user guidance

b) AGD_PRE.1 Preparative procedures

c) ALC_DEL.1 Delivery procedures

4.2. Assumptions

The ST provides additional information on the assumptions made and the threats countered.

Personnel Assumptions

1. It is assumed that one or more authorized administrators are assigned who are competent to manage the TOE and the security of the information it contains, trained for the secure operation of the TOE, and who can be trusted not to deliberately abuse their privileges so as to undermine security.
2. It is assumed that authorized TOE users are trusted to correctly install, configure and operate the TOE according to the instructions provided by the TOE documentation.
3. It is assumed that there will be no untrusted users and no untrusted software on the TOE component servers.

Physical Assumptions

1. It is assumed that the TOE components critical to the security policy enforcement will be protected from unauthorized physical modification.

Intended Usage Assumptions

1. It is assumed that those responsible for the TOE will ensure the communications between the TOE components and between the TOE components and remote users are configured to use secure channels.
2. It is assumed that those responsible for the TOE will ensure that data stored in the databases used by the TOE will be protected from unauthorized access via the Operational Environment interfaces.
3. It is assumed that those responsible for the TOE will ensure executable and data files used by the TOE will be protected from unauthorized access via the Operational Environment interfaces.
4. It is assumed that users will protect their authentication data.
5. It is assumed that the host computer on which the HostInfo Agent has been installed has been configured to allow the agent to collect the data the TOE needs

for risk and compliance assessment (i.e. the assessment scripts are able to "see" the necessary data).

4.3. Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (EAL 2 in this case).
2. This evaluation only covers the specific version of the product identified in this document, and not any earlier or later versions released or in process.
3. As with all EAL 2 evaluations, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
4. The TOE is intended to be operated in a system high environment where all data is controlled to the highest level of security classification assigned to the operating environment.
5. Not all cryptographic functions used by the TOE have been FIPS certified. The correctness of these cryptographic modules used by the TOE is by Vendor assertion; the correctness and conformance of these modules to any standard will not be part of this evaluation. Those cryptographic functions used for trusted communication between TOE components have been FIPS certified (RSA BSafe Crypto-J v3.6 JSafe Software Module (cert #812) and JCE Provider Module (cert #820). See Section 1.4.6 of the ST for details of the cryptographic functions.
6. The correctness and conformance of the templates to any government or commercial standard is by Vendor assertion. Verifying the correctness and conformance of the templates to any standard, the correctness of the assessment scripts for the assessment task, or that the process steps defined by the templates are complete and sufficient will not be part of this evaluation.
7. Security classification markings that can be configured via the administrative functions for projects and documents are for advisory purposes only. The TOE and its underlying databases are single-level applications that do not separate data based on any label or classification. The TOE is *not* a multi-level security (MLS) product. No enforcement of any kind is based off of this label.
8. The following are included in the Physical Scope of the Evaluation:
    - Xacta IA Manager: Assessment Engine (Assessment Engine)
        - Assessment Engine Application Server
        - Dashboard

- Publishing Server
- Third party subsystems included as part of the AE that are installed with the TOE:
  - Tomcat 5.5.27
  - JRE 6 update 13
  - iReasoning SNMP Subagent Service v1
  - Bouncy Castle 1.40
  - RSA BSafe Crypto-J v3.6 (JSafe and JCE)

  Note: The supplied Tomcat/Apache and JRE are installed by the TOE's installation process and are instantiations that are only available for use by the TOE and must not be upgraded by the customer.

- Xacta IA Manager: Continuous Assessment (Xacta Continuous Assessment)
  - Asset Manager
  - Asset Manager GUI
  - Detect Server
  - Detect Server GUI
  - HostInfo Agents
  - Third party subsystems included as part of the AM and DS installed with the TOE:
    - Tomcat 5.5.27
    - JRE 6 update 13
    - iReasoning SNMP Subagent Service v1
    - Bouncy Castle 1.40
    - RSA BSafe Crypto-J v3.6 (JSafe and JCE)

    Note: The supplied Tomcat/Apache and JRE are installed by the TOE's installation process and are instantiations that are only available for use by the TOE and must not be upgraded by the customer.

- Default Government or Commercial Templates included with the product

  Note: The correctness and conformance of the templates to any government or commercial standard is by Vendor assertion. Verifying the correctness and conformance of the templates to any standard, the correctness of the assessment scripts for the assessment task, or that the process steps defined by the templates are complete and sufficient is not part of this evaluation.

- Default Test Scripts included with the product

- JavaScript Extensions

  Note: The assessment scripts with the JavaScript Extensions defined in the Xacta® JavaScript Extensions Reference Manual for Version 4.0, Service Pack 8, June 15 2009 were tested for basic functionality and that the results provided by scripts were used by the AE's risk assessment process.

9. The following are not included in the Physical Scope of the Evaluation:

   The following components of the Xacta IA Manager V4.0 SP8 framework is separately licensed and is not included in the TOE:

   - Xacta IA Manager: Process Enforcer
   - Legacy HostInfo Agents (previous agents from earlier versions of the TOE).

   The following product subsystems are used for installation and maintenance and are not included in the TOE:

   - HostInfo Utility
   - HostInfo Agent Configuration Utility
   - Xacta Utilities GUI

   The following are Operational Environment components that are excluded from the scope of the evaluation:

   - None of the underlying operating system (OS) software and hardware of the TOE component's (servers and agents) host platforms
   - Underlying third-party relational databases (including the MS SQL Express 2005 that is packaged with the product)
   - MS Office (MS Word must be completely installed for the Publishing Server)
   - .NET framework (.NET 2.0 is included with the product, but will only be installed if there is not a version 2.0 or better .NET framework installed.
   - WinPcap driver 4.1.1 (The customer must pre-install this driver and use the version included with the product. This must not be updated by the customer as the WinPcap drivers must undergo integration testing with the TOE.)
   - SSL capable Web Browser installed on any platform being used as an Administrative Console
   - Third-party applications used to view TOE output (e.g. MS Word, MS Excel, OpenOffice, or Adobe Acrobat). (These applications do not come with the product and must be separately installed by the customer.)
   - LDAP or Active Directory Server (optional)
   - SMTP Server (optional)
   - SNMP Network Management Station/Server (optional)

- Syslog Server (optional)
- Third-party Asset Discovery/Vulnerability Scanners/ Enterprise Management Databases (optional)
    - Nessus (Version 2.0)
    - eEye Retina / REM (Retina 5.x with REM Event server 3.6)
    - ISS Internet Scanner (7.0 SP2)
    - ISS Site Protector (Version)
    - Microsoft SMS (2003 Server)
    - IBM Tivoli (Version)
- Public Key Infrastructure components (includes any drivers needed for operation)
    - Card Reader for Common Access Cards (CAC)
    - Certificate Authorities
- Network Infrastructure
- Protocol Implementations

10. The Security Functions listed in Section 3 of this document are included in the Logical Scope of the Evaluation.
11. The following functionality is not included in the Logical Scope of the Evaluation:
    - Use of deprecating Xacta Automated Script Language (XASL).
    - Correctness and modification of Velocity scripts to publish and customize reports.
    - Publisher Component's use of the velocity scripts and the data provided by the AE to correctly and accurately publish the report(s) (i.e the functionality to generate a report is in scope just not the verification that the report is correct and/or accurate).
    - Verification of the correctness and completeness of the
        - project templates to meet claimed standard
        - process steps assigned to the project templates
        - assigned assessment scripts to the process steps
        - published reports to meet selected C&A submittal requirements for claimed standards
    - Correctness, modification, customization, or creation of the individual assessment scripts (TOE's ability to assign, execute, and retrieve results from scripts is in scope).

- Verification of the Job Scheduler to correctly invoke scheduled jobs at the times configured
- WYSIWYG Editor
- System of Systems configuration (hierarchical deployment of AE servers)
- Project Control Implementation Inheritance application feature.
- Verification of the correctness and completeness of the imported SCAP or OVAL assessment scripts.
- Use of security classification markings

  Note: Security classification markings are only used to display a visual reminder of the highest classification level of data that should be stored in the application.

5. Architectural Information

Xacta technologies are database driven Web applications that are supported by Tomcat/Apache web services and the Java Runtime Environment (JRE) that is packaged with the product. The supplied Tomcat/Apache and JRE are installed by the TOE's installation process and are instantiations that are only available for use by the TOE.

The TOE is a software-only product whose components and external interfaces are shown in Figure 1 below. The physical boundary of the TOE is the Assessment Engine and Continuous Assessment components of the Xacta IA Manager V4.0 SP8 framework as commercially available from the developer.

The TOE is intended to be operated in a system high environment where all data is controlled to the highest level of security classification assigned to the operating environment.

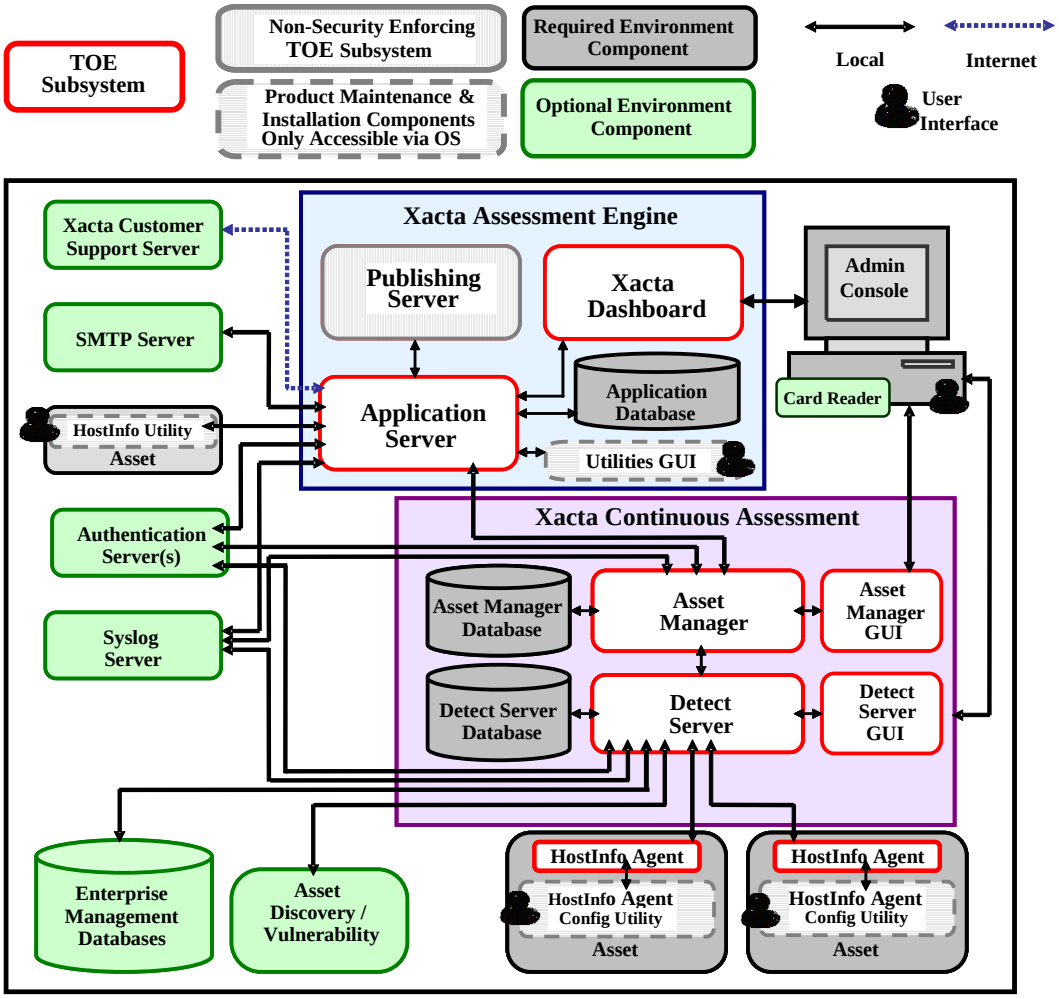

Figure 1: Xacta IA Manager: Assessment Engine and Xacta IA Manager: Continuous Assessment Components and Interfaces

The Xacta IA Manager TOE is comprised of the following components and subsystems:

5.1. Xacta IA Manager: Assessment Engine (AE)

The Assessment Engine component consists of software designed to facilitate IT security risk and compliance assessment business functions, such as supporting the data collection and document publishing for a Certification & Accreditation approval process. It consists of the following subsystems described below:

Security Enforcing TOE Subsystems:

- **Xacta Assessment Engine Application Server (Application Server)**

  The Application Server subsystem provides the core business logic of the application. As such, all other Xacta IA Manager subsystems communicate with the Application Server. The Application Server analyzes the collected IT network asset information and calculates risk and compliance with the requirements derived from the administratively selected template.

  The following steps summarize the basic Xacta IA Manager workflow:

  a) A project is started with the selection of a template

  b) The project's tasks are assigned to individuals who have designated roles

  c) The collection and assessment tasks are performed (either automatically and/or manually)

  d) Documents are published from the resulting task data for the project

  e) The operational environment of the project can then be continuously monitored, updated, and re-assessed for deviations

  The Application Server maintains data in a centralized database (Application Database). This data includes:

  - An organization's baseline risk posture and configuration information
  - TOE user account information, audit records, and system configuration data
  - Snapshots that are backup copies of a project that can be used to restore the project to an earlier state
  - Published documents

  The Application Database's records are automatically updated when a risk element file is imported.

  This data maintained by the Application Server in actuality a database instance (schema and data) inside a third-party RDBMS. This RDBMS, the I&A and access control functionality it provides, and its interfaces, though used by the TOE, are not controlled by the TOE. Therefore, the I&A and access control functionality to the third-party RDBMS are specified in the Operational Environment objectives.

As part of the installation, a database can be created to be used to contain the Application Server data or an existing database instance may be used. Some of the database settings may be changed through the Dashboard's management functions.

An encrypted SSL channel is required for communications between the Application Server and the database even if they are installed on the same server. The database must be specially configured in order to enable this encryption.

- **Xacta Dashboard (Dashboard)**

  The Dashboard is a web based graphical user interface through which all management functions for the Assessment Engine are accessed. This interface is used by all account holders for administration purposes. The Dashboard is accessed via a standard web browser, such as Internet Explorer. The Dashboard consists of server-side application software.

Non-Security Enforcing TOE Subsystems:

- **Xacta Publishing Server (Publishing Server or Publisher)**

  Because it does back-end publishing tasks for Assessment Engine, the Publisher is considered a non-security relevant component; all security features are handled by Assessment Engine. Although the Publisher is included in the TOE, it does not enforce any security functionality and is included only for completeness.

  The Publishing Server is used by Assessment Engine to generate C&A documentation. It produces documents in either Adobe portable document format (.pdf) or Microsoft Word format (.doc). The final documentation package can then be submitted to a Designated Approving Authority (DAA). These documents are the essential part of the formal work product associated with a security certification and accreditation effort.

Product Subsystems Not Included in the TOE:

The following subsystems are product utilities used only by customers during the installation, initial configuration, and maintenance of the TOE. They are not used during the run-time operation of the TOE and their functionality is not part of the TOE Security Functionality. Users of these utilities must have physical access to the platform on which they are installed. Identification and authentication of users of these utilities is done by the OS of the platform. The TOE does not audit use of the utilities.

- **Xacta HostInfo Utility (HostInfo Utility)**

  The HostInfo Utility is used to manually retrieve host information from Windows assets. Data obtained by the HostInfo Utility can be saved to a file, zipped, and imported into Assessment Engine's Equipment Inventory process step.

  The HostInfo Utility is executed from the target machine's command prompt. Therefore the HostInfo Utility user must have physical access to the Assessment Engine server and a login account on the target machine's OS.

- **Xacta Utilities GUI**

This utility is automatically installed during installation and can be accessed from the Windows task bar under *Start > Programs > Xacta > Xacta Utilities*. The Xacta Utilities GUI user must have physical access to the Assessment Engine server and a login account on the server's OS. The main utility screen provides access to the utilities associated with each of the installed components and subsystems. The following utilities are available through the GUI:

- **Application File Digest Checker Utility**

  This utility calculates the checksum for the program files and then compares the results with a list from Xacta or with previous scan results generated by the utility to enables customers to verify the authenticity and integrity of their Xacta software.

- **Certificate Management Utility**

  The Certificate Management Utility (CMU) helps create and manage Java-standard keystores, their private keys, and certificates. This includes the ability to generate self-signed certificates, import existing certificates and key pairs, and migrate a certificate, and replace a self-signed certificate with one duly signed by a trusted Certificate Authority (CA).

- **Database Management Utility**

  The Database Management Utility is exclusive for the Assessment Engine. This utility lets customers perform entire backups, restore from backups, and update the password encryption for the database.

- **Publisher SNMP Utility**

  The Publisher SNMP Utility allows customers to configure the TOE's SNMP subagent to report to a master SNMP agent.

- **Web Server Configuration Utility**

  The Assessment Engine Web Server Configuration Utility lets customers switch between Non-SSL and SSL protocol and change the URL of the Assessment Engine Web server.

5.2. Xacta IA Manager: Continuous Assessment (Continuous Assessment)

The Continuous Assessment component is a set of integrated subsystems designed to automate risk and compliance assessment business functions. It includes the subsystems described below.

Security Enforcing TOE Subsystems:

- **Xacta Asset Manager (Asset Manager)**

  The Asset Manager is a service that enables the management of an enterprise's IT network assets. It is a Web-based application that automatically collects and updates data about network devices, creates and maintains an asset inventory, tests asset configurations and vulnerabilities, and generates detailed reports. The

Asset Manager provides the Assessment Engine with up-to-date host and vulnerability data as part of the assessment process.

The Asset Manager maintains data in its own database instance (Asset Manager Database) consisting of collected asset information, script results, and data from third-party asset discovery/vulnerability scanners for assets in its associated Detect Server(s) specified IP Range.

- **Xacta Detect Server (Detect Server)**

  The Detect Server is responsible to manage a configured set of assets (hosts with HostInfo agents). When the Asset Manager Server has a task, it sends it to the appropriate Detect Server.

  Depending on the type of task to be performed, the Detect Server either executes it by itself or passes it on to the HostInfo Agents. When the task is complete, the Detect Server passes the information back to the Asset Manager Server.

  Detect Servers can perform network discovery scans or request data from third-party enterprise management tools such as Microsoft SMS, IBM Tivoli, ISS Site Protector, eEye REM, and Nessus. Detect Servers can request detailed equipment scans and vulnerability tests from HostInfo Agents.

  Each Detect Server can only perform scans on equipment within its specified IP Range and will only accept HostInfo Agents within this range. The IP Range limit is specified when the Detect Server is configured. Multiple Detect Servers may be configured to be used in a single installation.

  Each Detect Server maintains data in its own database instance (Detect Server Database) consisting of collected asset information, script results, and data from third-party asset discovery/vulnerability scanners for assets in the Detect Server's specified IP Range. Each Detect Server's database records are replicated within the Asset Manager Database on a near real-time basis. The synchronization of this data is a function of the Asset Manager and Detect Server subsystems.

  The Continuous Assessment databases (Asset Manager Database and Detect Server Databases) are similar in implementation to the database used by the Application Server. These are two database instances (schema and data) inside a third-party RDBMS. This RDBMS, the I&A and access control functionality it provides, and its interfaces, though used by the TOE, are not controlled by the TOE. Therefore, the I&A and access control functionality to the third-party RDBMS are specified in the Operational Environment objectives.

- **Asset Manager and Detect Server GUIs**

  The Asset Manager and the Detect Servers each have their own associated web based graphical user interface used by all account holders for administration purposes. These GUIs act similarly to the Dashboard, however the management functions and information displayed in each pertain only to the appropriate Asset Manager or Detect Server.

The Asset Manager and Detect Server GUIs are accessed via a standard web browser, such as Internet Explorer. Each Asset Manager and Detect Server GUI has its own individual web pages and a unique URL.

- **Xacta HostInfo Agent (HostInfo Agent)**

  A HostInfo Agent is an application that resides on a host computer (IT network asset). The agent is designed to collect detailed data about its host and transmit it back to the Detect Server using encrypted Secure Sockets Layer (SSL) protocol. The agent can also run tests on its host.

  Agents are designed to periodically contact the Detect Server to see if updated information is required about the agent's host. If updated information is required, the agent performs the Detect Server's requested task, passes the resulting information back to the server, and returns to idle mode.

  HostInfo Agents produce a log file that can be configured and read through the OS utilities of its host. This log file is used for diagnostics and debugging but could contain audit information that would be valuable to the administrator.

Product Subsystems Not Included in the TOE:

The following subsystems are product utilities used only by customers during the installation, initial configuration, and maintenance of the TOE. They are not used during the run-time operation of the TOE and their functionality is not part of the TOE Security Functionality. Users of these utilities must have physical access to the platform on which they are installed. Identification and authentication of users of these utilities is done by the OS of the platform. The TOE does not audit use of the utilities.

- **HostInfo Agent Configuration Utility**

  This utility provides a graphical user interface that allows customers to start and stop agents, and configure all major agent properties. This utility is installed on each asset as part of the agent installation.

- **Xacta Utilities GUI**

  The Xacta Utilities GUI is also available on the Asset Manager Server in a distributed configuration. The Xacta Utilities GUI user must have physical access to the Asset Manager Server and a login account on the server's OS.

6. Documentation

Note: Documents shown in **bold** are delivered to the end user with the product. The notation "[builds]" refers to the following:

Assessment Engine Build 22212
Asset Manager Build 4974
Detect Server Build 3249
Hostinfo-Windows (32-bit) Build 1875
Hostinfo-Windows (64-bit) Build 1875
Hostinfo-Mac Build 1793
Hostinfo-Unix (Solaris and Red Hat) Build 1878

6.1. Guidance Documentation

The following documents are developed and maintained by the Vendor and delivered to the end user of the TOE:

[1] **Xacta® IA Manager: Assessment Engine™ Reference Manual Version 4.0, Service Pack 8, December 21, 2009**

[2] **Xacta® IA Manager: Assessment Engine™ Version 4.0, Service Pack 8 Release Notes [builds], December 10, 2009**

[3] **Xacta® IA Manager: Continuous Assessment™ Reference Manual Version 4.0, Service Pack 8, December 21, 2009**

[4] **Xacta® IA Manager: Continuous Assessment™ Version 4.0, Service Pack 8 Release Notes [builds] 7 December 10, 2009**

[5] **Secure Installation & Configuration Supplement For Xacta® IA Manager: Assessment Engine and Xacta® IA Manager: Continuous Assessment, Version 4.0 Service Pack 8 (Commercial and Government Distribution Packages), [builds], Version 4.1, 23 July, 2010**

[6] **Xacta® JavaScript Extensions Reference Manual for Version 4.0, Service Pack 8, June 15, 2009**

6.2. Security Target (ST)

Security Target (ST)

[1] Security Target for Xacta® IA Manager: Assessment Engine and Xacta® IA Manager: Continuous Assessment, Version 4.0 Service Pack 8 (Commercial and Government Distribution Packages) [builds], Version 2.1, July 30, 2010

6.3. Development (ADV) Evidence Documentation

[1] Security Architecture (EAL2) for Version 4.0 Service Pack 8 Xacta® IA Manager: Assessment Engine And Xacta® IA Manager: Continuous Assessment, [builds], Version 2.1, July 23, 2010. [Telos Proprietary]

[2] Security Functional Specification for Version 4.0 Service Pack 8 Xacta® IA Manager: Assessment Engine And Xacta® IA Manager: Continuous Assessment, [builds], Version 2.1, July 23, 2010. [Telos Proprietary]

[3] Total Design of the System for Version 4.0 Service Pack 8 Xacta® IA Manager: Assessment Engine And Xacta® IA Manager: Continuous Assessment, [builds], Version 2.1, September 8, 2010. [Telos Proprietary]

6.4. Life-Cycle (ALC) Evidence Documentation

[1] Configuration Management Process for Version 4.0 SP8 Xacta IA Manager: Assessment Engine And Xacta IA Manager: Continuous Assessment, [builds], V 2.1, July 23, 2010 [Telos Proprietary]

[2] Delivery Procedures for Version 4.0 SP8 Xacta® IA Manager: Assessment Engine And Xacta® IA Manager: Continuous Assessment, [builds], Version 2.1, July 23, 2010 [Telos Proprietary]

[3] Flaw Remediation for Xacta IA Manager: Assessment Engine and Xacta IA Manager: Continuous Assessment Version 4.0 SP8, [builds], Version 2.1, July 23, 2010 [Telos Proprietary]

6.5. Testing (ATE) and Vulnerability Analysis (AVA) Documentation

[1] AVA Search Results Assessed_v3 (2).docx

[2] Coverage Mapping Xacta (March 04 2010).xls

[3] Security Test Plan for Xacta® IA Manager Version 4.0 SP8, [builds], Version 2.1, July 23, 2010 [Telos Proprietary]

[4] EAL2 On-Site Test Report For Xacta® IA Manager: Assessment Engine and Xacta® IA Manager: Continuous Assessment, Version 4.0 Service Pack 8 (Commercial and Government Distribution Packages), [builds], Version 1.2, July 23, 2010. [Cygnacom and Xacta Proprietary]

6.6. Evaluation Technical Report (ETR)

[1] Evaluation Technical Report For a Target of Evaluation Volume 1: Evaluation of the ST for Xacta® IA Manager with Continuous Assessment Version 4.0 Service Pack 8, [builds], ST Version 2.1, Version 1.6, September 8, 2010 [Cygnacom Proprietary]

[2] Evaluation Technical Report For a Target of Evaluation Volume 2: Evaluation of the TOE for Xacta® IA Manager with Continuous Assessment Version 4.0 Service Pack 8, [builds], ST Version 2.1, Version 1.6, September 8, 2010 [Cygnacom Proprietary]

7. IT Product Testing

At EAL 2, the overall purpose of the testing activity is "independently testing a subset of the TSF, whether the TOE behaves as specified in the design documentation, and to gain confidence in the developer's test results by performing a sample of the developer's tests." (ATE_IND.2, 14.6.2.1 [CEM])

At EAL 2, the developer's test evidence must "show the correspondence between the tests provided as evaluation evidence and the functional specification. However, the coverage analysis need not demonstrate that all TSFI have been tested, or that all externally-visible interfaces to the TOE have been tested. Such shortcomings are considered by the evaluator during the independent testing." (ATE_COV.1, 14.3.1.3 [CEM])

This section describes the testing efforts of the vendor and the evaluation team.

The objective of the evaluator's independent testing sub-activity is "to demonstrate that the security functions perform as specified. Evaluator testing includes selecting and repeating a sample of the developer tests." (ATE_IND.2, Independent testing – sample [CC])

Note: Not all cryptographic functions used by the TOE have been FIPS certified. The correctness of these cryptographic modules used by the TOE is by Vendor assertion; the correctness and conformance of these modules to any standard was not part of this evaluation. The following functions use the FIPS certified RSA BSafe Crypto-J v3.6 JSafe Software Module (cert #812) or JCE Provider Module (cert #820):

- *Local Password Storage*
- *External Authentication Server Data Storage*
- *3rd Party Application Password Storage*
- *Data transmitted between AE and Publisher*
- *Communications between TOE Components*
- *Communications between TOE and External Servers*
- *Communications between TOE and Xacta Customer Support Server*
- *Communications between TOE and network assets*
- *Project Backup and Restore*

For the other functions, the cryptography has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation.

7.1. Developer Testing

The developers took the following approach for the development of their functional tests:

1. Define the features that needed to be tested based on the security function descriptions from the TSS section of the ST.

2. Define the features that needed to be tested based on the FSP.
3. Create tests for each security function to ensure coverage of that particular function.
4. Design each test to stand test and be reproducible at any time.

The goal of the developer testing was ensure that the functions work as described in the ST and FSP and to uncover any defects.

The developer tests were incorporated into the Vendor's normal QA process. The software testing life cycle is made up of six phases: Planning, Analysis, Design, Test Cycles/Bug Fixes, Final Testing and Implementation, and Post Implementation.

The developer's test plan identifies what was expected to receive a pass verdict:

- All processes need to execute without unexpected errors.
- All processes must finish update/execution in an acceptable amount of time based on benchmarks provided by the business analysts and documented by the development team.

The test plan called for defects to be tracked by a software program called Silk Radar. Defects were noted and corrected, and the relevant test was rerun. This cycle was executed until the problem is resolved.

The TOE was installed in standalone mode with external support platforms for the operational environment components, such as the SMTP server, Vulnerability scanner, and an Oracle DBMS. The platforms were installed on their test network.

The outcome of the developer testing was the successful completion of the tests as documented in the test plan.

The vendor resubmitted test results as a result of product upgrades and fixes for defects during the course of the evaluation.

Each set of test results was verified by the evaluator and documented in the Coverage Mapping Xacta (March 31 2010).xls spreadsheet. The evaluator looked at the test run, build, date, results, correctness of results, and the individual who signed off on the test to determine satisfactory test results.

All developer tests were run at least once, while most tests were run at least 3 times. The vendor documented failures and unexpected results and those tests were rerun until they passed.

The evaluator determined that the developer's approach to testing the TSFs was adequate for an EAL2 evaluation.

7.2. Evaluator Independent Testing

Independent testing was performed at the vendor's location Ashburn VA. Testing was conducted by the evaluator from March 17, 2010 to March 24, 2010.

Installation of the TOE

The Assessment Engine (AE), Asset Manager (AM), and Detect Server (DS) are web Java applications that are designed to be platform independent. Therefore, the evaluator chose to run a sampling on the different Microsoft Windows platforms. The following table is a summary of which operating systems were used for the components during the total test effort.

Summary of platform testing (I – IND testing, D- Developer testing based on evidence):

		AE	AM	DS	HostInfo
Vista		I	Equiv	Equiv	I
Server 2003		D	D & I	D & I	D
XP-32		I	I	I	D & I
XP-64		n/a	n/a	n/a	I
Mac		n/a	n/a	n/a	I
Red Hat		n/a	n/a	n/a	I
Solaris 10		n/a	n/a	n/a	Equiv

The Unix HostInfo agent is universally packaged (i.e., one build number). The operational code itself is the same. The only difference would be the environmental items such as pointers to file structures. Therefore, security testing on Red Hat would be the equivalent of testing on Solaris 10.

The evaluator's installation of the TOE was slightly different than developer's configuration. The developer's testing used a standalone configuration (i.e. everything on the same host machine) and the evaluator has chosen to test on a standard network configuration.

- One of the design aspects (or claims) of the TOE is that the product's encrypted communications between TOE components behaves the same whether installed in standalone or a distributed environment. This claim can be verified by choosing to install the TOE in a distributed environment and re-running the encrypted communications tests that the developer's used. Assuming that this claim is true the developer's environment and the Evaluator's chosen environment are equivalent.
- This configuration also allows the evaluator to verify that TOE components do operate correctly in Vista and 2003 Server. The developer used XP. This would cover all three advertised operating systems. Any test run should run the same and have the same results no matter what OS the component is running on.

Installation Results:

- The documented steps for the AE installation were specified incorrectly. Updates to the Vendor documentation were made.

- The installation procedures were updated to correct the deficiencies discovered during the AM and DS installation. The new installation manual was successfully tested.
- All TOE identification references displayed were consistent with the CM documentation
- Once the TOE was completely installed, it was examined and found to be in the state described in the Vendor's user guides.
- The file digest results for the TOE's executable program files were incorrectly documented. A fix for this problem has been implemented and documented by the Vendor.
- An error in MS SQL 2005 Express required a workaround. This required setting an environment variable.
- Since MS SQL 2005 Express is an outdated product, instructions about how to get patches were included in the customer documentation.

Execution of the Developer's Functional Tests

The evaluator reran more than 50% of the developer's tests; the tests selected provided more than 90% results coverage. Several tests had areas of duplication that could be used to verify the security function without having to specifically rerun the test (for example password masking, audit generation review). New features and those tests that were not run by the developer on the final build (based on their development process) were given highest priority in the selection process. Tests were conducted on Assessment Engine, Asset Manager, Detect Server, and Agents. It was the intent of the evaluator to interact with all human interfaces and stimulate some of the external interfaces including the optional SMTP server interface, Vulnerability Scanner, Syslog, and/or LDAP. The set of developer tests run by the evaluator is listed in the evaluator's test report.

Results:

- All but one of the developer tests rerun by the evaluator passed. In response to the failure, the developer removed a user role (Unrestricted User) for the AE. This cleaned up the confusion of the defined user roles. The ST and TDS were updated. The developer's user manuals were updated after it was discovered that they missed a couple of references to the deprecated roles.

Team-Defined Functional Tests

The evaluator also selected/designed tests for the purpose of ensuring that all interfaces tested to a sufficient depth and to ensure that all interfaces have been stimulated and that the reactions to the stimulation are what where expected based on the FSP. The supplemental (team-defined) tests run by the evaluator along with their purpose and basic description are listed in the evaluator's test report.

Results:

- All Team-Defined Functional Tests ran successfully.

Penetration Testing

The evaluator used a Nessus scanner to conduct the following scans at the following intervals:

- Prior to installing TOE software (determine baseline of OS)
- After installing TOE software (determine what the TOE opened/closed/changed)
- Beginning of new day of testing (verify that TOE hasn't changed due to testing or manipulation of TOE overnight)
- At the end of testing. (verify that TOE is still in appropriate state after testing)

The evaluator also ran the ad-hoc penetration tests as documented in the evaluator's test report.

Results:

- Only the Microsoft SQL Server showed high risk vulnerabilities as a result of the Nessus scans. The patches were applied to remove the vulnerabilities. Installation supplement was updated to reflect the need for the patches for the incorporated version of Microsoft SQL Server Express.
- One low level vulnerability finding resulted in a recommendation to upgrade to newer Crypto-J FIPS implementation for future releases:
    - The SSL certificate that has been signed using a cryptographically weak hashing algorithm - MD2, MD4, or MD5.
- Another notable low level vulnerability identified was the "remote service allows renegotiation of TLS / SSL connections" notice. It was discovered that this is vulnerability is introduced by the Tomcat and JRE environments (6 update 17 or earlier). Telos narrowed the vulnerability to the JRE environment. One recommendation found was to use a firewall to protect the OE from this kind of external attack. Telos's project plan for the TOE includes keeping the product current with the third party software such as JRE and Tomcat. The JRE and Tomcat had already been updated as a result of this evaluation.

8. Evaluated Configuration

The evaluated configuration of the TOE covers both the standalone deployment (Assessment Engine and Continuous Assessment components installed on one machine) *and* standard network deployment (Assessment Engine separately installed from Continuous Assessment components). Figure 1 depicts the standard network deployment. The following are the builds evaluated:

- AE build #: 22212
- AM build #: 4974
- Detect build #: 3249
- HostInfo Agent Windows 32-bit build #: 1875
- HostInfo Agent Windows 64-bit build #: 1875
- HostInfo Agent Fedora build #: 1878
- HostInfo Agent Solaris build #: 1878
- HostInfo Mac build #: 1793

The main TOE components Assessment Engine Server, Asset Manager, and the Detect Server were installed on the following Microsoft OSs: XP, Vista, Server 2003.

The HostInfo Agent was installed on: Vista, Server 2003, XP, Mac OS X, Red Hat Linux, and Solaris 10.

The relational databases that were used: MS SQL Express 2005, MS SQL Server 2005, Oracle 10g (tested by developer only).

MS Word 2003 & 2007

MS .NET 3.5 SP1

Identification and Authentication was provided by the TOE's native password protection, LDAP PKI authentication, CAC provided certificates, and Windows Domain authentication.

Provided and installed by the TOE:

- JRE 6 update 13
- Tomcat 5.5.27

Provided by the TOE:

- WinPcap 4.1.1

Administrative Console

- Windows XP or Vista
- SSL capable Web Browser used: IE7, IE8, Firefox 3.6.0, Firefox 3.6.2
- Adobe Acrobat Reader 9.3

Special configuration requirements for CC configuration:

- The “madmin” account must be disabled after another account with madmin capabilities is created.
- The AM must be configured to only send signed scripts to the HostInfo Agent.
- The HostInfo Agents must be configured to only execute signed scripts.

Other items installed on a separate server/platform(s) as part of the Operational Environment that were not part of the TOE included the following:

- LDAP and Active Directory Server (including public key infrastructure)
- SMTP Server
- Syslog Server
- Xacta Customer Service Center Server (https://customers.xacta.com)
- Asset Discovery/Vulnerability Scanners / Enterprise Management Databases:
    - Nessus (2.0)
    - eEye Retina / REM (Retina 5.10 with Event Server 3.6)
    - ISS Internet Scanner (7.0 SP2)
    - ISS Site Protector – not used
    - Microsoft SMS (2003 Server)
    - IBM Tivoli – not used

9. Results of Evaluation

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon version 3.1 R2 of the CC and the CEM.

The Evaluation Team assigned a pass, fail, or inconclusive verdict to each work unit of each EAL 2 assurance component. For fail or inconclusive work unit verdicts, the Evaluation Team advised the developer of issues requiring resolution or clarification within the evaluation evidence. In this way, the Evaluation Team assigned an overall pass verdict to the assurance component only when all of the work units for that component had been assigned a pass verdict.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by CygnaCom CCTL.

Below lists the assurance requirements the TOE was required meet to be evaluated and pass at Evaluation Assurance Level 2 augmented with ALC_FLR.2. The following components are taken from CC part 3. The components in the following section have no dependencies unless otherwise noted.

- ADV_ARC.1 Security architecture description
- ADV_FSP.2 Security-enforcing functional specification
- ADV_TDS.1 Basic design
- AGD_OPE.1 Operational user guidance
- AGD_PRE.1 Preparative procedures
- ALC_CMC.2 Use of a CM system
- ALC_CMS.2 Parts of the TOE CM coverage
- ALC_DEL.1 Delivery procedures
- ALC_FLR.2 Flaw reporting procedures
- ASE_CCL.1 Conformance claims
- ASE_ECD.1 Extended components definition
- ASE_INT.1 ST Introduction
- ASE_OBJ.2 Security objectives
- ASE_REQ.2 Derived security requirements
- ASE_SPD.1 Security problem definition
- ASE_TSS.1 TOE summary specification
- ATE_COV.1 Evidence of coverage
- ATE_FUN.1 Functional testing

- ATE_IND.2 Independent testing – sample
- AVA_VAN.2 Vulnerability analysis

The evaluators concluded that the overall evaluation result for the target of evaluation is pass. The evaluation team reached PASS verdicts for all applicable evaluator action elements and consequently all applicable assurance components.

- The TOE is CC Part 2 Extended
- The TOE is CC Part 3 Conformant.
- The validators reviewed the findings of the evaluation team, and have concurred that the evidence and documentation of the work performed support the assigned rating.

10. Validators Comments/Recommendations

1. The product provides the ability to download SCAP Content Updates, including new and up-to-date CVE (Common Vulnerabilities and Exposures), CCE (Common Configuration Enumeration), and CPE (Common Platform Enumeration) data. As with Active Update, SCAP Content Update is disabled by default and may be configured to retrieve data either automatically or manually. Both the Continuous Assessment and Hostinfo agents are listed on the NIST website as being SCAP validated, for version 4.0 SP8 (which the website mistakenly lists as V4.8).
2. Although they are initialization tools, all of the Xacta Utilities were tested on both the AE and CA servers.
3. Although the product provides the ability to do printouts with classification markings, these markings must be considered **advisory only** as the product does not deal with labeled data nor run on a multilevel system. Under no circumstances should the markings be higher than the overall system classification.
4. The supplied scripts have not been evaluated as to suitability, correctness, or completeness for their claimed tasked. The scripting language has been evaluated to confirm that statements behave as claimed. Thus, if the scripts are written correctly, they will assess what they appear to assess.
5. The audit record for a failed login records the invalid username. Users should note this could mistakenly expose a password if a user mistakenly enters their password for a username.
6. The vendor has asserted (but it was not confirmed by the evaluation team) that the TOE can satisfy any of the standards against which it can assess. In particular, the vendor has indicated that they have customers using the product in a STIG-compliant environment.
7. The default number of character classes are insufficient to meet the requirements of IAIA-1 or IA-5(1) as completed by CNSS 1253. If those controls are applicable in the environment of use, the password character class value should be 4, and the history value should be 10. This is noted in the configuration guide.
8. It is the responsibility of administrators to use mechanisms in the operational environment to regularly backup audit records.
9. Note: Not all cryptographic functions used by the TOE have been FIPS certified. The correctness of these cryptographic modules used by the TOE is by vendor assertion; the correctness and conformance of these modules to any standard was not part of this evaluation. The following functions use the FIPS certified RSA BSafe Crypto-J v3.6 JSafe Software Module (cert #812) or JCE Provider Module (cert #820):
    - Local Password Storage
    - External Authentication Server Data Storage

- 3rd Party Application Password Storage
- Data transmitted between AE and Publisher
- Communications between TOE Components
- Communications between TOE and External Servers
- Communications between TOE and Xacta Customer Support Server
- Communications between TOE and network assets
- Project Backup and Restore

For the other functions, the cryptography has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation.

11. Security Target

The Security Target for Xacta® IA Manager: Assessment Engine and Xacta® IA Manager: Continuous Assessment, Version 4.0 Service Pack 8 (Commercial and Government Distribution Packages) is compliant with the Specification of Security Targets requirements found within Annex B of Part 1of the CC.

12. Glossary

12.1. Acronyms

The following are product specific and CC specific acronyms. Not all of these acronyms are used in this document.

ACI	Access Control Item
AE	Assessment Engine
AM	Asset Manager
AO	Authorizing Official
C&A	Certification and Accreditation
CA	Certificate Authority
CA	Continuous Assessment
CAC	Common Access Card
CC	Common Criteria [for IT Security Evaluation]
CCE	Common Configuration Enumeration
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology
CIDR	Classless Inter Domain Routing
CLI	Command Line Interface
CM	Configuration Management
CMU	Certificate Management Utility
CNSS	Committee on National Security Systems
COBIT	Control Objectives for Information and related Technology
CPE	Common Platform Enumeration
CRL	Certificate Revocation List
CSC	Customer Service Center
CVE	Common Vulnerabilities and Exposures
DAA	Designated Approving Authority
DBMS	Database Management System
DIACAP	DoD Information Assurance Certification and Accreditation Process

DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DCID	Director of Central Intelligence Directive
DoD	Department of Defense
DS	Detect Server
EAL	Evaluation Assurance Level
EMC²	Not an acronym—corporate brand
FIPS	Federal Information Processing Standards Publication
FSP	Functional Specification
FTP	File Transfer Protocol
GB	Gigabyte
GUI	Graphical User Interface
HTTP	HyperText Transmission Protocol
HTTPS	HyperText Transmission Protocol, Secure
IA	Information Assurance
IBM	International Business Machines
ICMP	Internet Control Message Protocol
IE	Internet Explorer
I&A	Identification and Authentication
IP	Internet Protocol
ISO	International Organization for Standardization
ISS	Internet Security Systems
JCE	Java™ Cryptography Extension
JRE	Java Runtime Environment
LDAP	Lightweight Directory Access Protocol
ID	Identifier
IT	Information Technology
JRE	Java Runtime Environment
JVM	Java Virtual Machine
MAC	Message Authentication Code
MD*n*	Message Digest
MS	Microsoft
NIAP	National Information Assurance Partnership

NIST	National Institute of Standards and Technology
OE	Operational Environment
OS	Operating System
OVAL	Open Vulnerability and Assessment Language
PDF	(Adobe) Portable Document Format
PKI	Public Key Infrastructure
PP	Protection Profile
QA	Quality Assurance
RDBMS	Relational Database Management System
REM	Product name. Part of the RETINA® Enterprise Suite
RSA	Rivest, Shamir and Adleman; corporate name for the security division of EMC^2
SCAP	Security Content Automation Protocol
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirements
SMS	Systems Management Server
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSL	Secure Sockets Layer
ST	Security Target
STIG	Security Technical Implementation Guides
TCP/IP	Transmission Control Protocol/Internet Protocol
TDS	TOE Design Specification
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TOE Security Functions Interface
TSP	TOE Security Policy
UDP	User Datagram Protocol
UI	User Interface
URI	Uniform Resource Identifier

URL	Uniform Resource Locator
VR	Validation Report
WYSIWYG	"What you see is what you get"
XASL	Xacta Automated Script Language
XP	Microsoft operating system
XML	Extensible Markup Language

12.2. Terminology

This section defines the product-specific and CC-specific terms. Not all of these terms are used in this document.

Agent	A HostInfo subsystem installed on a system on the target network that will automatically collect asset data (part of the Continuous Assessment Upgrade).
Artifact	An object, such as a file or a link to a Web site or Web document, that is included for reference within projects.
Asset	Any device connected to the target network with an IP address that is assessed by the TOE for risks and compliance to security standards.
Assignment	The specification of an identified parameter in a component.
Assurance	Grounds for confidence that an entity meets its security objectives.
Attack Potential	The perceived potential for success of an attack, should an attack be launched, expressed in terms of a threat agent's expertise, resources and motivation.
Augmentation	The addition of one or more assurance component(s) to a package.
Authentication Data	Information used to verify the claimed identity of a user.
Authorised User	A user who may, in accordance with the SFR, perform an operation.
Checklist	A high-level evaluation tool that can be used to quickly assess the overall compliance of a system.
Class	A grouping of families that share a common focus.
Component	The smallest selectable set of elements on which requirements may be based.

Connectivity	The property of the TOE that allows interaction with IT entities external to the TOE. This includes exchange of data by wire or by wireless means, over any distance in any environment or configuration.
Dependency	A relationship between components such that if a requirement based on the depending component is included in a PP, ST or package, a requirement based on the component that is depended upon must normally also be included in the PP, ST or package.
Element	An indivisible security requirement.
Evaluation	Assessment of a PP, an ST, or a TOE against defined criteria.
Evaluation Assurance Level	A package consisting of assurance components from Part 3 that represents a point on the CC predefined assurance scale.
Evaluation Authority	A body that implements the CC for a specific community by means of an evaluation scheme and thereby sets the standards and monitors the quality of evaluations conducted community.
Evaluation Scheme	The administrative and regulatory framework under which the CC is applied by an evaluation authority within a specific community.
Extension	The addition to an ST or PP of functional requirements not contained in Part 2 and/or assurance requirements not contained in Part 3 of the CC.
External Entity	Any entity (human or IT) outside the TOE that interacts (or may interact) with the TOE.
Family	A grouping of components that share security objectives but may differ in emphasis or rigor.
Folder	A logical grouping of projects.
Formal	Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.
Housekeeping	Background system maintenance performed by the TOE at an administrator scheduled time.
Identity	A representation (e.g. a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.
Informal	Expressed in natural language.

Inter-TSF Transfers	Communicating data between the TOE and the security functions of other trusted IT products.
Internal Communication Channel	A communication channel between separated parts of TOE.
Internal TOE transfer	Communicating data between separated parts of the TOE.
Iteration	The use of the same component to express two or more distinct requirements.
Keystore	A java file containing a trusted certificate and private key.
Knowledge Base	The policies, regulations, requirements, test procedures, vulnerabilities, and scripts needed by the TOE that are stored and updated.
Notification	A notification sent to the individual assigned to a project role upon the occurrence of a designated project event.
Object	A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.
Organizational Security Policies	A set of security rules, procedures, or guidelines imposed (or presumed to be imposed) now and/or in the future by an actual or hypothetical organization in the operational environment.
Package	A named set of either functional or assurance requirements (e.g. EAL 3).
Process Step	A key step within the assessment process; a component of a task.
Project	The representation of a system assessment effort; used to define the system, determine the requirements that must be complied with (template), gather system data, test the system, determine the overall level of compliance and the resulting risk, and prepare the documentation that will be submitted to the appropriate authorities for approval to operate.
Project Role	A set of project duties assigned to an individual to properly formatted documents.
Protection Profile	An implementation-independent statement of security needs for a TOE type.

Prove	This term refers to a formal analysis in its mathematical sense. It is completely rigorous in all ways. Typically, “prove” is used when there is a desire to show correspondence between two TSF representations at a high level of rigor.
Publishing	The process of compiling the data gathered from a project’s process steps and exporting it.
Refinement	The addition of details to a component.
Role	A predefined set of rules establishing the allowed interactions between a user and the TOE.
Scan Job	The automatic monitoring, updating, and testing of a project’s devices and equipment on a regular, recurring basis. (part of the Continuous Assessment Upgrade)
Secret	Information that must be known only to authorized users and/or the TSF in order to enforce a specific SFP.
Secure State	A state in which the TSF data are consistent and the TSF continues correct enforcement of the SFRs.
Security Attribute	A property of subjects, users (including external IT products), objects, information, sessions and/or resources that is used in defining the SFRs and whose values are used in enforcing the SFRs.
Security Function Policy	A set of rules describing specific security behavior enforced by the TSF and expressible as a set of SFRs.
Security Objective	A statement of intent to counter identified threats and/or satisfy identified organization security policies and/or assumptions.
Security Target	An implementation-dependent statement of security needs for a specific identified TOE.
Selection	The specification of one or more items from a list in a component.
Semiformal	Expressed in a restricted syntax language with defined semantics.
Snapshots	Backup copies of a project that can be used to restore the project to an earlier state.
Subject	An active entity in the TOE that performs operations on objects.

Target of Evaluation	A set of software, firmware and/or hardware possibly accompanied by guidance.
Task	A stage in the assessment process; a component of a project (selected template).
Template	The collection of work tasks that comprise a particular set of requirements; these tasks comprise the steps needed to gather and evaluate the asset data and publish documents; the templates are named after government and commercial standards that the product supports.
TOE Resource	Anything useable or consumable in the TOE.
TOE Security Functions	A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.
Transfers Outside TSF	TSF mediated communication of data to entities not under control of the TSF.
Trusted Channel	A means by which a TSF and a remote trusted IT product can communicate with necessary confidence.
Trusted Path	A means by which a user and a TSF can communicate with necessary confidence.
TSF Data	Data created by and for the TOE that might affect the operation of the TOE.
TSF Interface	A means by which external entities (or subjects in the TOE but outside of the TSF) supply data to the TSF, receive data from the TSF and invoke services from the TSF.
User	See **external entity**
User Data	Data created by and for the user that does not affect the operation of the TSF.
Velocity Scripts	A Java-based template engine. It can be used as a standalone utility for generating source code, HTML, reports, or it can be combined with other systems to provide template services.

13. Bibliography

URLs

[1] Common Criteria Evaluation and Validation Scheme (CCEVS): (http://www.niap-ccevs.org/cc-scheme).

[2] CygnaCom Solutions CCTL (http://www.cygnacom.com).

[3] Xacta IA Manager (http://www.telos.com/solutions/information%20assurance/xacta%20ia%20manager/)

CCEVS Documents

[1] Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, September 2006 Version 3.1 Revision 1, CCMB-2006-09-001.

[2] Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components, September 2007 Version 3.1 Revision 2, CCMB-2007-09-002.

[3] Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components, September 2007, Version 3.1 Revision 2, CCMB-2007-09-003.

[4] Common Methodology for Information Technology Security Evaluation - Evaluation methodology, September 2007, Version 3.1 Revision 2, CCMB-2007-09-004.