RSA®, The Security Division of EMC®

RSA Archer™ eGRC Platform v5.0

Security Target

Evaluation Assurance Level (EAL): EAL2+
Document Version: 0.6

Prepared for:

RSA®, The Security Division of EMC®
174 Middlesex Turnpike
Bedford, MA 01730
United States of America

Phone: +1 (877) 722-4900
Email: info@rsa.com
http://www.rsa.com

Prepared by:

Corsec Security, Inc.
13135 Lee Jackson Memorial Hwy., Suite 220
Fairfax, VA 22033
United States of America

Phone: +1 (703) 267-6050
Email: info@corsec.com
http://www.corsec.com

Table of Contents

1 INTRODUCTION 4
1.1 PURPOSE 4
1.2 SECURITY TARGET AND TOE REFERENCES 4
1.3 PRODUCT OVERVIEW 4
1.3.1 Platform Components 6
1.3.2 Reports and Dashboards 7
1.4 TOE OVERVIEW 8
1.5 TOE ENVIRONMENT 8
1.6 TOE DESCRIPTION 9
1.6.1 Physical Scope 9
1.6.2 Logical Scope 10
1.6.3 Product Physical/Logical Features and Functionality not included in the TSF 11

2 CONFORMANCE CLAIMS 12

3 SECURITY PROBLEM 13
3.1 THREATS TO SECURITY 13
3.2 ORGANIZATIONAL SECURITY POLICIES 13
3.3 ASSUMPTIONS 14

4 SECURITY OBJECTIVES 15
4.1 SECURITY OBJECTIVES FOR THE TOE 15
4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT 15
4.2.1 IT Security Objectives 15
4.2.2 Non-IT Security Objectives 15

5 EXTENDED COMPONENTS 17

6 SECURITY REQUIREMENTS 18
6.1.1 Conventions 18
6.2 SECURITY FUNCTIONAL REQUIREMENTS 18
6.2.1 Class FAU: Security Audit 20
6.2.2 Class FDP: User Data Protection 22
6.2.3 Class FIA: Identification and Authentication 23
6.2.4 Class FMT: Security Management 24
6.2.5 Class FMT: TOE Access 26
6.3 SECURITY ASSURANCE REQUIREMENTS 27

7 TOE SPECIFICATION 28
7.1 TOE SECURITY FUNCTIONS 28
7.1.1 Security Audit 29
7.1.2 User Data Protection 29
7.1.3 Identification and Authentication 29
7.1.4 Security Management 30
7.1.5 TOE Access 30

8 RATIONALE 31
8.1 CONFORMANCE CLAIMS RATIONALE 31
8.2 SECURITY OBJECTIVES RATIONALE 31
8.2.1 Security Objectives Rationale Relating to Threats 31
8.2.2 Security Objectives Rationale Relating to Policies 32
8.2.3 Security Objectives Rationale Relating to Assumptions 34
8.3 RATIONALE FOR EXTENDED SECURITY FUNCTIONAL REQUIREMENTS 35
8.4 RATIONALE FOR EXTENDED TOE SECURITY ASSURANCE REQUIREMENTS 35
8.5 SECURITY REQUIREMENTS RATIONALE 35
8.5.1 Rationale for Security Functional Requirements of the TOE Objectives 35

8.5.2 Security Assurance Requirements Rationale *38*
8.5.3 Dependency Rationale *38*

9 ACRONYMS **40**

Table of Figures

FIGURE 1 – RSA ARCHER EGRC PLATFORM V5.0 5
FIGURE 2 – RSA ARCHER EGRC PLATFORM V5.0 COMPONENTS 6
FIGURE 3 – PHYSICAL TOE BOUNDARY 9

List of Tables

TABLE 1 - ST AND TOE REFERENCES 4
TABLE 2 - CC AND PP CONFORMANCE 12
TABLE 3 - THREATS 13
TABLE 4 - ORGANIZATIONAL SECURITY POLICIES 14
TABLE 5 - ASSUMPTIONS 14
TABLE 6 - SECURITY OBJECTIVES FOR THE TOE 15
TABLE 7 - IT SECURITY OBJECTIVES 15
TABLE 8 - NON-IT SECURITY OBJECTIVES 16
TABLE 9 - TOE SECURITY FUNCTIONAL REQUIREMENTS 18
TABLE 10 - ASSURANCE REQUIREMENTS 27
TABLE 11 - MAPPING OF TOE SECURITY FUNCTIONS TO SECURITY FUNCTIONAL REQUIREMENTS 28
TABLE 12 - THREATS:OBJECTIVES MAPPING 31
TABLE 13 - POLICIES:OBJECTIVES MAPPING 32
TABLE 14 - ASSUMPTIONS:OBJECTIVES MAPPING 34
TABLE 15 - OBJECTIVES:SFRS MAPPING 35
TABLE 16 - FUNCTIONAL REQUIREMENTS DEPENDENCIES 38
TABLE 17 - ACRONYMS 40

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The TOE is the RSA Archer eGRC Platform v5.0, and will hereafter be referred to as the TOE throughout this document. This software-only TOE is a platform for building on-demand applications and packaging them into solutions that solve specific business needs.

1.1 Purpose

This ST is divided into nine sections, as follows:

- Introduction (Section 1) – Provides a brief summary of the ST contents and describes the organization of other sections within this document. It also provides an overview of the TOE security functions and describes the physical and logical scope for the TOE, as well as the ST and TOE references.
- Conformance Claims (Section 2) – Provides the identification of any Common Criteria (CC), ST Protection Profile, and Evaluation Assurance Level (EAL) package claims. It also identifies whether the ST contains extended security requirements.
- Security Problem (Section 3) – Describes the threats, organizational security policies, and assumptions that pertain to the TOE and its environment.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and its environment.
- Extended Components (Section 5) – Identifies new components (extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs)) that are not included in CC Part 2 or CC Part 3.
- Security Requirements (Section 6) – Presents the SFRs and SARs met by the TOE.
- TOE Specification (Section 7) – Describes the security functions provided by the TOE that satisfy the security functional requirements and objectives.
- Rationale (Section 8) – Presents the rationale for the security objectives, requirements, and SFR dependencies as to their consistency, completeness, and suitability.
- Acronyms (Section 9) – Defines the acronyms and terminology used within this ST.

1.2 Security Target and TOE References

Table 1 - ST and TOE References

ST Title	RSA®, The Security Division of EMC® RSA Archer™ eGRC Platform v5.0 Security Target
ST Version	Version 0.6
ST Author	Corsec Security, Inc.
ST Publication Date	September 20, 2011
TOE Reference	RSA Archer eGRC Platform v5.0, build 5.0.2.1130

1.3 Product Overview

The Product Overview provides a high level description of the product that is the subject of the evaluation. The following section, TOE Overview, will provide the introduction to the parts of the overall product offering that are specifically being evaluated.

The RSA Archer eGRC Platform supports business-level management of Enterprise Governance, Risk, and Compliance (eGRC). As the foundation for all RSA Archer eGRC Solutions, the Platform allows you to adapt the solutions to your requirements, build your own applications, and integrate with other systems without writing a single line of code.

Figure 1 – RSA Archer eGRC Platform v5.0

The RSA Archer eGRC Platform is:

- Flexible
  - The Platform offers a point-and-click interface for building and managing business applications. Non-technical users can automate processes, streamline workflow, control user access, tailor the user interface, and report in real-time.
- Unified
  - RSA provides a common platform to manage policies, controls, risks, assessments and deficiencies across lines of business. This unified approach eases system complexity, strengthens user adoption, and reduces training time.
- Collaborative
  - The Platform enables cross-functional collaboration and alignment. Business users across IT[1], finance, operations and legal domains can work together in an integrated framework using common processes and data.

A few of RSA Archer eGRC Platform v5.0's key features are:

- Rapid Application Development
  - Administrators can seize the power of the RSA Archer eGRC Platform to model hundreds of business processes in a fraction of the time it would take to develop traditional custom applications.
- Deployment Flexibility
  - Administrators can balance administrative control, time-to-value, and cost considerations when planning their implementation of the RSA Archer eGRC Platform.
- System Integration
  - Administrators can automate the movement of data into and out of the RSA Archer eGRC Platform to support data analysis, process management, and reporting.
- Archer eGRC Exchange

[1] IT: Information Technology

- Users can take advantage of pre-built applications and integrations for the RSA Archer eGRC Platform. They can test drive, download and deploy from the Archer eGRC Exchange.

1.3.1 Platform Components

The RSA Archer eGRC Platform offers a point-and-click interface for tailoring solutions, building new applications and integrating with external data sources. Non-technical users can automate business processes, streamline workflow, control user access, adapt the user interface and deliver real-time reports without relying on IT to accomplish their goals.

Figure 2 – RSA Archer eGRC Platform v5.0 Components

1.3.1.1 Application Builder

The Application Builder offers powerful tools and a user-friendly interface for building and tailoring business applications with no programming required. Administrators can design applications to capture and display any kind of data, and they have full control over the page layout, allowing them to create an intuitive experience for end users.

1.3.1.2 Reports and Dashboards

To gain value from the data, administrators need a comprehensive, real-time view of the business. Through the RSA Archer eGRC Platform, administrators can generate actionable reports that allow them to share data with other users and track the status of various initiatives. They can also build graphical, role-specific dashboards to monitor metrics across business units.

1.3.1.3 Access Control

To ensure the integrity of the business data and a streamlined user experience, administrators need to enforce access controls so users can interact only with the information that is appropriate for their roles. With powerful yet easy-to-use access control features, administrators can control information access at the system, application, record and field level.

1.3.1.4 User Experience

The RSA Archer eGRC Platform offers a simple interface for customizing the user's experience in the software, including branding applications with a corporate look and feel. Administrators are free to use

their unique company colors, graphics, icons and text to facilitate end-user adoption of new applications. Administrators can also embed custom instructions in the user interface to facilitate self-training and diminish the learning curve.

1.3.1.5 Notifications

The RSA Archer eGRC Platform allows administrators to automatically notify users via email when new information requires their attention, when tasks enter their queue, or when deadlines approach. To ensure that right users are alerted at the right time, RSA enables administrators to define simple or complex notification rules. Email notifications can also include direct links to the content that users need to take action or make a decision.

1.3.1.6 Business Workflow

Workflow capabilities allow administrators to define and automate business processes for streamlining the management of content, tasks, statuses, and approvals. Through the content review feature, administrators can route information to subject-matter experts for editing or authorization prior to sharing that data with a broader audience. RSA also enables administrators to assign tasks automatically based on data conditions within an application, eliminating manual task management processes.

1.3.1.7 Integration

The RSA Archer eGRC Platform allows seamless integration of cross-departmental and enterprise data systems through a variety of integration components. The Platform is designed to be both vendor neutral and content independent to support cross-system information gathering and consolidation.

1.3.2 Reports and Dashboards

When administrators build applications on the RSA Archer eGRC Platform to centralize, automate and manage business processes, they gain a comprehensive, real-time view of the enterprise. RSA's powerful reporting capabilities allow administrators to quickly generate reports that provide the information they need to make decisions, address issues, and complete tasks. RSA also enables them to build customizable dashboards tailored by audience so every user gets exactly the information they need depending on their roles and responsibilities.

1.3.2.1 Actionable Reporting

The RSA Archer eGRC Platform provides a user-friendly interface for performing simple keyword searches or complex, multi-application searches. On an ad hoc basis, administrators can generate reports that are filtered by business unit, geography, date range, or any other meaningful criteria. No matter the size of the data set, RSA provides the administrator with quick access to the specific information they need to make informed decisions.

RSA also makes it easy to share reports with other users, and because the Platform's reporting capabilities are real-time, reports will always display the latest information, allowing administrators to keep pace with the changing nature of the business.

1.3.2.2 Charts and Graphs

RSA's charting functionality enables administrators to graphically display projects by type, requests by priority, tasks by status, and any other data set that's meaningful to the business. Displaying a report as a chart or graph rather than text makes a strong visual impact on users and conveys a large data set in a concise space. This enables users to grasp the full scope of the data without paging through hundreds or thousands of records.

With RSA's drill-down capabilities, users can click any portion of a chart to view details of the underlying information, making the charts highly interactive. Because RSA's charting functionality is configurable, administrators have complete control over the size, color palette and labeling of the chart, allowing administrators to adhere to the company's design standards.

1.3.2.3 Powerful Dashboards

RSA's dashboard capabilities give administrators instant access to the real-time information they need to run the business. Dashboards display graphical and textual reports that allow them to monitor critical metrics across business units in a consolidated view.

Through the RSA Archer eGRC Platform, administrators can create user-specific dashboards to deliver key information to the right people at the right time. For example, administrators can provide executive leadership with graphical summary reports for any area of the business with the ability to drill in for more details. For managers who need information at the business-unit level, administrators can provide a real-time view of activities by date, person, status, priority, etc. RSA's dashboard capabilities also empower general users with easy access to tasks, requests and supporting information.

1.4 TOE Overview

The TOE Overview summarizes the usage and major security features of the TOE. The TOE Overview provides a context for the TOE evaluation by identifying the TOE type, describing the product, and defining the specific evaluated configuration.

The software-only TOE is the RSA Archer eGRC Platform v5.0 software. It comprises ASP.NET application code that runs on Microsoft Internet Information Services (IIS) on the Microsoft Windows Server family of operating systems (OS). The evaluated configuration targets the 32 and 64-bit editions of the TOE, running on multiple platforms. For Microsoft Windows 2003, IIS version 6.0 is used, along with Microsoft SQL Server 2005 for the TOE database. For Windows 2008, IIS 7.x is used, along with SQL Server 2008 for the database. The OS, web server, and database server software are excluded from the TOE boundary. An external LDAP[2] server in the TOE environment is required to support identification and authentication with external user accounts. Microsoft Windows Active Directory is the product used in the evaluated configuration.

The TOE is managed by authorised administrators through a web interface accessed via a user's web browser. To access the functions available via the web interface, an authorised administrator must open a web browser and enter the IP[3] address or hostname of the Archer server. Internet Explorer 7 is the browser used in the evaluated configuration. Communication between the web browser on the user and management workstations and the TOE is protected using a Transport Layer Security (TLS) connection provided by the underlying IIS server.

The TOE software provides a platform on which administrators can create task-specific applications. Users can then be assigned permission to access these applications in order to do their work. Administrators can design the applications to implement very granular control over their functions and data in order to granularly restrict and control user operations within the applications.

1.5 TOE Environment

The TOE is intended to be deployed on a secure Windows Server-based server in a secure data center that protects physical access to the TOE. The TOE is intended to be connected to a network that allows users to access the TOE server in a secure manner and that prevents malicious attackers from accessing the TOE. A Microsoft Active Directory server is installed in the TOE environment to support external user authentication.

[2] LDAP: Lightweight Directory Access Protocol
[3] IP: Internet Protocol

1.6 TOE Description

This section primarily addresses the physical and logical components of the TOE included in the evaluation.

1.6.1 Physical Scope

Figure 3 illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE and the constituents of the TOE Environment.

The essential physical components for the proper operation of the TOE in the evaluated configuration are:

- TOE software,
- server hardware and operating system (not included in the TOE boundary),
- network (not included in the TOE boundary),
- management workstation (not included in the TOE boundary), and
- LDAP server (not included in the TOE boundary).

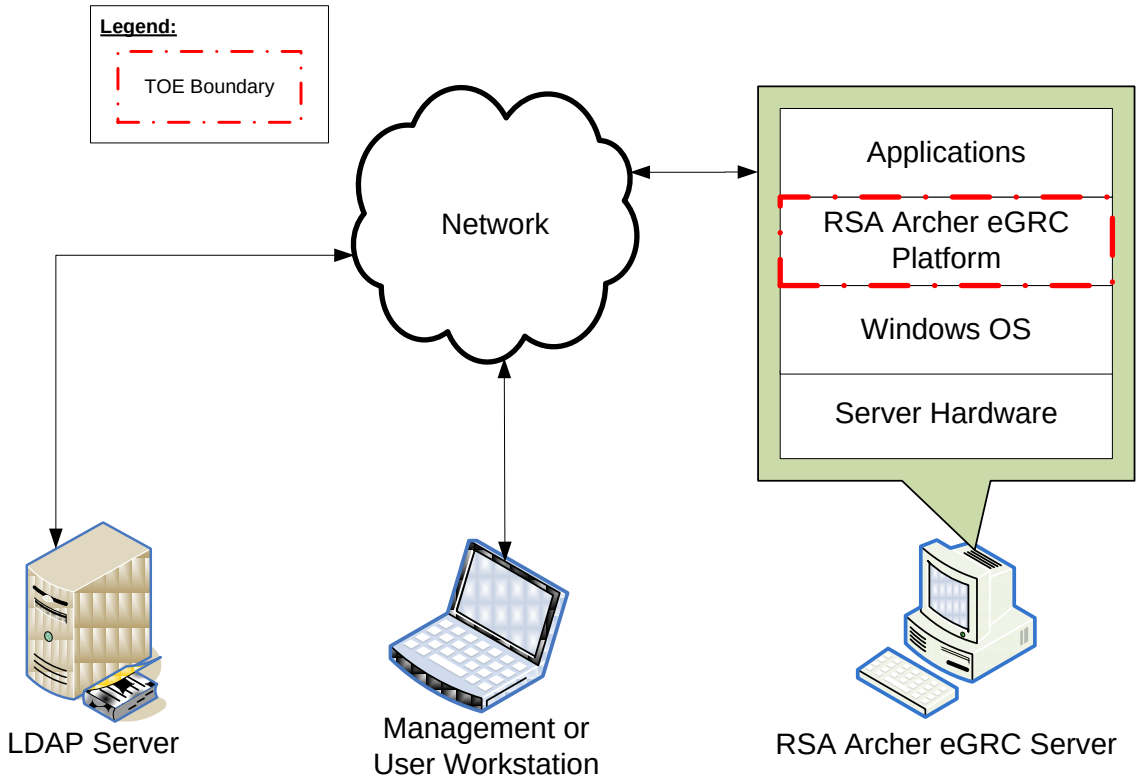

Figure 3 – Physical TOE Boundary

1.6.1.1 TOE Software

The TOE is a software-only TOE meant to be used with commercial off the shelf server hardware and the Windows Server-family of operating systems.

1.6.1.2 Guidance Documentation

The following guides are required reading and part of the TOE:

- Administrator Guide Online Help File
- User Guide Online Help File

- Control Panel Online Help File
- Installation Guide
- Web Services API[4] Guide
- Release Notes
- Common Criteria Guidance Documentation Supplement

1.6.2 Logical Scope

The TOE logical boundary is defined by the security functions that it implements. The security functions implemented by the TOE are usefully grouped under the following Security Function Classes:

- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management
- TOE Access

1.6.2.1 Security Audit

The TOE generates audit records for all login events, security events, and events recorded by applications executed by the TOE, including changes to application ownership, application content deletion, and updates to audited content records. The TOE also provides administrators with the ability to review and filter security events.

1.6.2.2 User Data Protection

The User Data Protection function implements functionality necessary to protect applications that are stored on and executed by the TOE. Users of the TOE are identified and authenticated, either by the TOE or the TOE Environment. These users are then granted appropriate access to applications and application functions managed and controlled by the TOE. Each user and application is associated with security attributes that determine which users can perform what operations on which applications.

1.6.2.3 Identification and Authentication

This function of the TOE is used to identify and authenticate each operator of the TOE. Users and administrators of the TOE can be authenticated directly by the TOE or can be authenticated by a separate LDAP server. Users and administrators are assigned one-to-many roles which determine what they are allowed to do within the TOE. This functionality is configured by an administrator.

The evaluated configuration consists of both locally administered user accounts and accounts synchronized with an external LDAP server. The TOE includes Single Sign-On support to bypass authentication for LDAP-authenticated users. A Windows domain controller running Active Directory will be used as the remote LDAP server in the evaluated configuration.

1.6.2.4 Security Management

The Security Management functionality of the TOE specifies several aspects of management of the TOE Security Function (TSF). Proper management of the TSF is required to properly mediate access to applications executed by the TOE.

The TOE is managed by authorised administrators via the web interface.

The Security Management function provides administrators with the ability to properly manage and configure the TOE to store and execute applications. Administrators are assigned one-to-many roles that determine which aspects of the TOE they are authorised to manage.

[4] Application Programming Interface

1.6.2.5 TOE Access

The TOE Access security function allows administrators to set a default security access banner, or disclaimer, that is displayed to end users prior to identification and authentication. The TOE's default configuration contains a blank value for the disclaimer field; therefore it must be configured in order to be compliant with the stated SFR.

1.6.3 Product Physical/Logical Features and Functionality not included in the TSF

No features or functionality are excluded from the evaluated configuration of the TOE.

2 Conformance Claims

This section provides the identification for any CC, Protection Profile (PP), and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. Rationale for CC and PP conformance claims can be found in Section 8.1.

Table 2 - CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009; CC Part 2 conformant; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations of the CEM as of 2010-10-30 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None.
Evaluation Assurance Level	EAL2+ augmented with Flaw Remediation (ALC_FLR.2).

3 Security Problem

This section describes the security aspects of the environment in which the TOE will be used and the manner in which the TOE is expected to be employed. It provides the statement of the TOE security environment, which identifies and explains all:

- Known and presumed threats countered by either the TOE or by the security environment
- Organizational security policies with which the TOE must comply
- Assumptions about the secure usage of the TOE, including physical, personnel and connectivity aspects

3.1 Threats to Security

This section identifies the threats to the IT assets against which protection is required by the TOE or by the security environment. The threat agents are divided into two categories:

- Attackers who are not TOE users: They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings or parameters and no physical access to the TOE.
- TOE users: They have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings or parameters and physical access to the TOE. (TOE users are, however, assumed not to be willfully hostile to the TOE.)

Both are assumed to have a low level of motivation. The IT assets requiring protection are the TSF[5] and user data saved on or transitioning through the TOE. Removal, diminution, and mitigation of the threats are achieved through the objectives identified in Section 4 Security Objectives. The following threats are applicable:

Table 3 - Threats

Name	Description
T.CONFIG	The TOE could be misconfigured to enforce improper access to user data.
T.MASQUERADE	A user or process could masquerade as another entity in order to gain unauthorized access to data or TOE resources.
T.UNAUTH	An unauthorized user could access data stored by the TOE by bypassing the protection mechanisms of the TOE.

3.2 Organizational Security Policies

An Organizational Security Policy (OSP) is a set of security rules, procedures, or guidelines imposed by an organization on the operational environment of the TOE. The following OSPs are presumed to be imposed upon the TOE or its operational environment by any organization implementing the TOE in the CC evaluated configuration:

[5] TSF – TOE Security Functionality

Table 4 - Organizational Security Policies

Name	Description
P.INTEGRITY	Data collected and produced by the TOE must be protected from modification.
P.MANAGE	The TOE may only be managed by authorized users.
P.PASSWORD	An authorized TOE user must use a sound password to access the TOE. A user password must have a minimum password length of eight characters and must contain at least one non-alphanumeric character (from a set of 33), one numeric character (from a set of 10), and two alphabetical characters (from a set of 52, since upper- and lowercase characters are differentiated).

3.3 Assumptions

This section describes the security aspects of the intended environment for the evaluated TOE. The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user guidance. The following specific conditions are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Table 5 - Assumptions

Name	Description
A.COMMSECURE	The IT environment provides the secure protocols necessary to protect the communication path between the TOE, end users, and the remote authentication server from unauthorised use or disclosure.
A.INSTALL	The TOE is installed on the appropriate hardware and operating system.
A.LOCATE	The TOE is located within a controlled access facility.
A.MANAGE	There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance.
A.PROTECT	The TOE software will be protected from unauthorized modification.
A.TIMESTAMP	The IT environment provides the TOE with the necessary reliable timestamps.

4 Security Objectives

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition (see Section 3). The set of security objectives for a TOE form a high-level solution to the security problem. This high-level solution is divided into two part-wise solutions: the security objectives for the TOE, and the security objectives for the TOE's operational environment. This section identifies the security objectives for the TOE and its supporting environment.

4.1 Security Objectives for the TOE

The specific security objectives for the TOE are as follows:

Table 6 - Security Objectives for the TOE

Name	Description
O.ADMIN	The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges (and only those TOE users) may exercise such control.
O.AUDIT	The TOE must record events of security relevance at the "not specified level" of audit. The TOE must record the resulting actions of the security functional policies and provide the authorized administrators with the ability to review the audit trail, and allow filtering to easily find information to aid in an investigation of a security violation.
O.AUTHENTICATE	The TOE must identify and authenticate users prior to allowing access to TOE administrative functions and data. The TOE must only allow authorized users to access appropriate TOE functions and data.
O.ACCESS	The TOE must present the user with a security disclaimer prior to identification and authentication to the TOE.
O.SELFPROTECT	The TOE must protect itself and its platform content from unauthorized access and tampering.

4.2 Security Objectives for the Operational Environment

4.2.1 IT Security Objectives

The following IT security objectives are to be satisfied by the environment:

Table 7 - IT Security Objectives

Name	Description
OE.COMMSECURE	The TOE environment must provide a secure communication path between the TOE, end users of the TOE, and the external authentication server in the TOE environment.
OE.PLATFORM	The TOE hardware and OS must support all required TOE functions.

Name	Description
OE.PROTECT	The TOE environment must protect itself and the TOE from external interference or tampering.
OE.TIME	The TOE environment must provide reliable timestamps to the TOE.

4.2.2 Non-IT Security Objectives

The following non-IT environment security objectives are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Table 8 - Non-IT Security Objectives

Name	Description
NOE.MANAGE	Sites deploying the TOE will provide competent TOE administrators who will ensure the system is used securely.
NOE.NOEVIL	Sites using the TOE shall ensure that TOE administrators are non-hostile, appropriately trained, and follow all administrator guidance.
NOE.PHYSICAL	The TOE will be used in a physically secure site that protects it from interference and tampering by untrusted subjects.

5 Extended Components

There are no extended SFRs or extended SARs for this evaluation of the TOE.

6 Security Requirements

This section defines the SFRs and SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.1.

6.1.1 Conventions

There are several font variations used within this ST. Selected presentation choices are discussed here to aid the Security Target reader.

The CC allows for assignment, refinement, selection and iteration operations to be performed on security functional requirements. All of these operations are used within this ST. These operations are performed as described in Part 2 of the CC, and are shown as follows:

- Completed assignment statements are identified using [*italicized text within brackets*].
- Completed selection statements are identified using [underlined text within brackets].
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement.
- Extended Functional and Assurance Requirements are identified using "EXT_" at the beginning of the short name.
- Iterations are identified by appending a letter in parentheses following the component title. For example, FAU_GEN.1(a) Audit Data Generation would be the first iteration and FAU_GEN.1(b) Audit Data Generation would be the second iteration.

6.2 Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 9 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 9 - TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_GEN.1	Audit Data Generation	✓	✓		
FAU_GEN.2	User identity association				
FAU_SAR.1	Audit review		✓		
FAU_SAR.2	Restricted audit review				
FAU_SAR.3	Selectable audit review		✓		
FDP_ACC.1	Subset access control		✓		
FDP_ACF.1	Security attribute based access control		✓		
FIA_UAU.2	User authentication before any action				
FIA_UID.2	User identification before any action				
FIA_AFL.1	Authentication failure handling	✓	✓		
FMT_MOF.1	Management of security functions behaviour	✓	✓		
FMT_MSA.1	Management of security attributes	✓	✓		
FMT_MSA.3	Static attribute initialisation	✓	✓		
FMT_MTD.1	Management of TSF data	✓	✓		

Name	Description	S	A	R	I
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓		
FTA_TAB.1	TOE access banner				
FTA_SSL.3	TSF-initiated termination		✓		

Note: S=Selection; A=Assignment; R=Refinement; I=Iteration

6.2.1 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 events:*
    a. Access Role Created/Deleted/Modified
    b. Audited Application Content Record Updated
    c. Account Status Modified
    d. Application Owner Added/Deleted
    e. Failed User Login
    f. Full Application Content Delete
    g. Global Report Permissions Granted/Removed
    h. LDAP Configuration Delete Started/Completed
    i. Maximum Login Retries Exceeded
    j. Password Changed by Administrator/User
    k. Role Assigned/Removed to/from User
    l. Security Parameter Assignment Modified
    m. Security Parameter Created/Deleted/Modified
    n. Sub-Form Owner Added/Deleted
    o. User Account Added/Deleted/Modified
    p. User Added/Removed to/from Group
    q. User Full Name Modified
    r. User Login
    s. User Login Name Modified
    t. User Logout

].

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 (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*no other audit relevant information*].

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.2 User identity association
Hierarchical to: No other components.
FAU_GEN.2.1

For audit events resulting from actions of identified users, 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 [*authorised users*] with the capability to read [*audit information for which they have been authorised*] 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 apply [*filtering*] of audit data based on [*security event types and time-based criteria*].

Dependencies: FAU_SAR.1 Audit review

6.2.2 Class FDP: User Data Protection

FDP_ACC.1 Subset access control
Hierarchical to: No other components.
FDP_ACC.1.1

The TSF shall enforce the [*Discretionary Access Control SFP*[6]] on
[
a) Subjects: TOE Users
b) Objects: Applications
c) Operations: Create, Read, Update, Delete
].

Application note: the Objects are applications created on and executed by the TOE.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACF.1 Security attribute based access control
Hierarchical to: No other components.
FDP_ACF.1.1

The TSF shall enforce the [*Discretionary Access Control SFP*] to objects based on the following:
[
Subject attributes:
1. *Username*
2. *Roles*
3. *Groups*
4. *Security Parameters*

Object Attributes:
1. *Object identifier*
].

FDP_ACF.1.2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
[
A valid subject of the TOE is allowed to perform create, read, update, or delete operations within an application if the subject has a role or group association which grants the appropriate permission.
].

FDP_ACF.1.3

The TSF shall explicitly authorise access of subjects to objects based on ~~the following~~ **no** additional rules: [~~assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*~~].

FDP_ACF.1.4

The TSF shall explicitly deny access of subjects to objects based on **no additional rules** ~~the~~ [~~assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*~~].

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

[6] SFP – Security Functional Policy

6.2.3 Class FIA: Identification and Authentication

FIA_UAU.2 User authentication before any action
Hierarchical to: FIA_UAU.1 Timing of authentication
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_UID.2 User identification before any action
Hierarchical to: FIA_UID.1 Timing of identification
FIA_UID.2.1
The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
Dependencies: No dependencies

FIA_AFL.1 Authentication failure handling
Hierarchical to: No other components
FIA_AFL.1.1
The TSF shall detect when [an administrator configurable positive integer within [*1 and 99*]] unsuccessful authentication attempts occur related to [*all authentication events*].
FIA_AFL.1.2
When the defined number of unsuccessful authentication attempts has been [met], the TSF shall [*temporarily deactivate the user account associated with the failed authentication attempts for a period of time defined as an administrator configurable positive integer within a range of 1 to 999 minutes, hours or days*].

Dependencies: FIA_UID.1 Timing of identification

6.2.4 Class FMT: Security Management

FMT_MOF.1 Management of security functions behaviour
Hierarchical to: No other components.
FMT_MOF.1.1

The TSF shall restrict the ability to [determine the behaviour of, disable, enable, modify the behaviour of] the functions:
[
Management of:

1. *users and groups*
2. *roles*
3. *security parameters*
4. *access control*
5. *applications*
6. *authentication behavior*
7. *notifications*
8. *login banner*
9. *data feeds*
10. *user workspaces/dashboards*
11. *forums*
12. *API integration*

]
to [*authorised administrators and users*].

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.1 Management of security attributes
Hierarchical to: No other components.
FMT_MSA.1.1

The TSF shall enforce the [*Discretionary Access Control SFP*] to restrict the ability to [change_default, query, modify, delete, [*create*]] the security attributes [*all security attributes*] to [*appropriately authorised roles*].

Dependencies: [FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.3 Static attribute initialisation
Hierarchical to: No other components.
FMT_MSA.3.1

The TSF shall enforce the [*Discretionary Access Control SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2

The TSF shall allow the [*authorised 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, [*create*]] the [*security attributes and applications*] to [*authorised administrators*].

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

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 management functions:

[

a) Management of security functions behavior;
b) Management of TSF data;
c) Management of security attributes

].

Dependencies: No Dependencies

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1

The TSF shall maintain the roles

[

a) "System Administrator"
b) Other roles created by the System Administrator or other appropriately privileged roles

].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

6.2.5 Class FMT: 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.

FTA_SSL.3 TSF-initiated termination
Hierarchical to: No other components
FTA_SSL.3.1
The TSF shall terminate an interactive session after a [*number of minutes, days or hours of user inactivity that is defined as an administrator configurable positive integer within a range of 1 to 99*].

Dependencies: No dependencies.

6.3 Security Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL2++ augmented with ALC_FLR.2. Table 10 - Assurance Requirements summarizes the requirements.

Table 10 - Assurance Requirements

Assurance Requirements	
Class ASE: Security Target evaluation	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
Class ALC : Life Cycle Support	ALC_CMC.2 Use of a CM[7] system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_FLR.2 Flaw reporting procedures
Class ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

[7] CM – Configuration Management

7 TOE Specification

This section presents information to detail how the TOE meets the functional requirements described in previous sections of this ST.

7.1 TOE Security Functions

Each of the security requirements and the associated descriptions correspond to the security functions. Hence, each function is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions satisfy the necessary requirements.

Table 11 - Mapping of TOE Security Functions to Security Functional Requirements

TOE Security Function	SFR ID	Description
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User identity association
	FAU_SAR.1	Audit review
	FAU_SAR.2	Restricted audit review
	FAU_SAR.3	Selectable audit review
User Data Protection	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
Identification and Authentication	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
	FIA_AFL.1	Authentication failure handling
Security Management	FMT_MOF.1	Management of security functions behaviour
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
TOE Access	FTA_TAB.1	TOE access banner
	FTA_SSL.3	TSF-initiated termination

7.1.1 Security Audit

The TOE generates audit records for startup and shutdown of the audit function, user login/logout events, security events, and events recorded by applications executed by the TOE. Audit records contain the date and time of the event, the type of event, subject identity (if applicable). The outcome of the event is not explicitly recorded; rather it is implied by the event type. For example, a "Failed Login" event implies a failed outcome. Authorised administrators can view the audit records via the web interface. Audit records are presented to administrators in a clearly readable and understandable format, and can be filtered via the web interface.

TOE Security Functional Requirements Satisfied: FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.2, and FAU_SAR.3.

7.1.2 User Data Protection

7.1.2.1 Discretionary Access Control SFP

The TOE also provides the User Data Protection security function to manage user interactions with applications that are executed by the TOE. Applications can be written to perform a variety of tasks for innumerable reasons, and the TOE ensures that users are not allowed to read application code and data, write or modify application code and data, and execute specific application tasks unless they have been properly authorised to do so.

Using the Security Management security function, Administrators of the TOE can configure the TOE and its applications to provide various functionality to end users. The TOE determines which users are allowed to access which portions of which applications (and to perform which operations) via a user's associated *username*, *security parameter*, *roles*, and *groups*. The username is the user's unique identifier within the TOE. A security parameter is a package of granular user-specific security settings (such as hours during which this particular user is allowed to log in). Roles are sets of associations with specific data within the TOE and its applications – a user must have the appropriate role in order to access specific data. Groups are associations of users with roles – a group is assigned one-to-many roles, and users are assigned one-to-many groups.

TOE Security Functional Requirements Satisfied: FDP_ACC.1, FDP_ACF.1.

7.1.3 Identification and Authentication

The TOE performs identification and authentication of both TOE administrators and end-users. The purpose of the identification and authentication function is to allow the TOE to restrict access to both administrative functions and to applications based upon the authenticated identity and associated attributes of a user.

Both administrators and users can access the TOE's management interface through a web browser. The TOE supports internally enforced username and password-based authentication as well as authentication with accounts that have been synchronized with an LDAP authentication server. Additionally, the TOE supports Single Sign-On, which passes authentication requests directly to the remote LDAP server. The first action that operators must take when attempting to interact with the TOE is to provide a username and password. Before identification and authentication, the TOE operator is not able to perform any TOE-mediated security functionality.

To protect itself from unauthorised access and tampering, the TOE automatically locks user accounts after an administrator-defined number of unsuccessful authentication attempts. The account remains locked until unlocked by an administrator, or after a period of time has lapsed, which is also configured by an administrator.

TOE Security Functional Requirements Satisfied: FIA_UAU.2, FIA_UID.2, and FIA_AFL.1.

7.1.4 Security Management

TOE administrators are responsible for managing and configuring the TOE. This includes managing applications executed by the TOE (including creating or installing them, maintaining them, and deleting them); managing the set of TOE users and administrators, roles, groups, and security parameters; and managing the permissions of users to access applications.

Administrators and users of the TOE are assigned to either the non-modifiable "System Administrator" role, or one or more of the roles created by an administrator.

TOE Security Functional Requirements Satisfied: FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1, and FMT_SMR.1.

7.1.5 TOE Access

The TOE is capable of displaying a default security warning regarding unauthorised use on the authentication page; however, the TOE's default configuration includes a blank value for the disclaimer field. In order to be compliant with the TOE Access SFR, an administrator must populate this field with custom security warning message text from the Archer Control Panel, as instructed by the *RSA Archer eGRC Platform 5.0 Guidance Documentation Supplement.*

The TOE also provides a mechanism which will expire user session after a period of inactivity. This period is defined by an authorised administrator.

TOE Security Functional Requirements Satisfied: FTA_TAB.1, FTA_SSL.3.

8 Rationale

8.1 Conformance Claims Rationale

This Security Target conforms to Part 2 and Part 3 of the Common Criteria Standard for Information Technology Security Evaluations, version 3.1 revision 3.

8.2 Security Objectives Rationale

This section provides a rationale for the existence of each threat, policy statement, and assumption that compose the Security Target. Sections 8.2.1, 8.2.2, and 8.2.3 demonstrate the mappings between the threats, policies, and assumptions to the security objectives are complete. The following discussion provides detailed evidence of coverage for each threat, policy, and assumption.

8.2.1 Security Objectives Rationale Relating to Threats

Table 12 - Threats:Objectives Mapping

Threats	Objectives	Rationale
T.CONFIG The TOE could be misconfigured to enforce improper access to user data.	O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges (and only those TOE users) may exercise such control.	O.ADMIN ensures that the TOE provides efficient management of its functions and data, mitigating the threat of accidental misconfiguration.
	O.AUTHENTICATE The TOE must identify and authenticate users prior to allowing access to TOE administrative functions and data. The TOE must only allow authorized users to access appropriate TOE functions and data.	O.AUTHENTICATE ensures that the TOE has identified and authenticated a user before he is allowed to access any data.
T.MASQUERADE A user or process could masquerade as another entity in order to gain unauthorized access to data or TOE resources.	OE.PROTECT The TOE environment must protect itself and the TOE from external interference or tampering.	OE.PROTECT prevents session spoofing by protecting data transferred between the TOE and its users from eavesdropping.
	O.AUTHENTICATE The TOE must identify and authenticate users prior to allowing access to TOE administrative functions and data. The TOE must only allow authorized users to access appropriate TOE functions and data.	O.AUTHENTICATE ensures that The TOE is able to identify and authenticate users prior to allowing access to TOE administrative functions and data.

Threats	Objectives	Rationale
T.UNAUTH An unauthorized user could access data stored by the TOE by bypassing the protection mechanisms of the TOE.	O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges (and only those TOE users) may exercise such control.	O.ADMIN ensures that access to TOE security data is limited to those users with access to the management functions of the TOE.
	O.AUDIT The TOE must record events of security relevance at the "not specified level" of audit. The TOE must record the resulting actions of the security functional policies and provide the authorized administrators with the ability to review the audit trail, and allow filtering to easily find information to aid in an investigation of a security violation.	O.AUDIT ensures that unauthorized attempts to access the TOE are recorded.
	O.AUTHENTICATE The TOE must identify and authenticate users prior to allowing access to TOE administrative functions and data. The TOE must only allow authorized users to access appropriate TOE functions and data.	O.AUTHENTICATE ensures that users are identified and authenticated prior to gaining access to TOE security data.
	O.ACCESS The TOE must present the user with a security disclaimer prior to identification and authentication to the TOE.	O.ACCESS ensures that unauthorized users are presented with a warning.
	O.SELFPROTECT The TOE must protect itself and its platform content from unauthorized access and tampering.	O.SELFPROTECT ensures that the TOE contains self-protection mechanisms that prevent unauthorized access.

Every Threat is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives counter all defined threats.

8.2.2 Security Objectives Rationale Relating to Policies

Table 13 - Policies:Objectives Mapping

Policies	Objectives	Rationale
P.INTEGRITY	O.AUDIT	O.AUDIT ensures that the TOE

Policies	Objectives	Rationale
Data collected and produced by the TOE must be protected from modification.	The TOE must record events of security relevance at the "not specified level" of audit. The TOE must record the resulting actions of the security functional policies and provide the authorized administrators with the ability to review the audit trail, and allow filtering to easily find information to aid in an investigation of a security violation.	will generate audit records of any attempt to change TOE or user data.
	OE.PROTECT The TOE environment must protect itself and the TOE from external interference or tampering.	OE.PROTECT ensures that the TOE's IT environment will protect the TOE from tampering.
	OE.TIME The TOE environment must provide reliable timestamps to the TOE.	OE.TIME ensures that TOE-generated audit records contain reliable timestamps.
P.MANAGE The TOE may only be managed by authorized users.	O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges (and only those TOE users) may exercise such control.	O.ADMIN ensures that the TOE provides the necessary tools to support the P.MANAGE policy.
	O.AUTHENTICATE The TOE must identify and authenticate users prior to allowing access to TOE administrative functions and data. The TOE must only allow authorized users to access appropriate TOE functions and data.	O.AUTHENTICATE ensures that only authorized users are granted access to the tools required to manage the TOE.
P.PASSWORD An authorized TOE user must use a sound password to access the TOE. A user password must have a minimum password length of eight characters and must contain at least one non-alphanumeric character (from a set of 33), one numeric character (from a set of 10), and two alphabetical characters (from a set of 52, since upper- and lowercase characters are differentiated).	O.AUTHENTICATE The TOE must identify and authenticate users prior to allowing access to TOE administrative functions and data. The TOE must only allow authorized users to access appropriate TOE functions and data.	O.AUTHENTICATE ensures that the TOE implements an identification and authentication mechanism robust enough to provide secure and robust identification and authentication of users.

Every policy is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives enforce all defined policies.

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 14 - Assumptions:Objectives Mapping

Assumptions	Objectives	Rationale
A.COMMSECURE The IT environment provides the secure protocols necessary to protect the communication path between the TOE, end users, and the remote authentication server from unauthorised use or disclosure.	OE.COMMSECURE The TOE environment must provide a secure communication path between the TOE, end users of the TOE, and the external authentication server in the TOE environment.	OE.COMMSECURE satisfies this assumption, by ensuring that TLS support is provided by the underlying IIS web server environment, as well as being implemented by the LDAP server, protecting any TSF or user data being transmitted between network entities.
A.INSTALL The TOE is installed on the appropriate hardware and operating system.	OE.PLATFORM The TOE hardware and OS must support all required TOE functions.	OE.PLATFORM ensures that the TOE hardware and OS supports the TOE functions.
A.LOCATE The TOE is located within a controlled access facility.	NOE.PHYSICAL The TOE will be used in a physically secure site that protects it from interference and tampering by untrusted subjects.	Physical security is provided within the TOE environment to provide appropriate protection to the network resources. NOE.PHYSICAL satisfies this assumption.
A.MANAGE There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.	NOE.MANAGE Sites deploying the TOE will provide competent TOE administrators who will ensure the system is used securely.	NOE.MANAGE satisfies the assumption that competent individuals are assigned to manage the TOE and the TSF.
A.NOEVIL The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance.	NOE.NOEVIL Sites using the TOE shall ensure that TOE administrators are non-hostile, appropriately trained, and follow all administrator guidance.	NOE.NOEVIL ensures that the sites deploying the TOE will provide only non-hostil, appropriately trained administrators that follow all administrator guidance.
A.PROTECT The TOE software will be protected from unauthorized modification.	OE.PROTECT The TOE environment must protect itself and the TOE from external interference or tampering.	The TOE environment provides protection from external interference or tampering. OE.PROTECT satisfies this assumption.
	NOE.PHYSICAL The TOE will be used in a physically secure site that protects it from interference and tampering by untrusted subjects.	NOE.PHYSICAL ensures that the TOE's IT environment protects the TOE from interference and tampering by untrusted subjects.
	O.SELFPROTECT The TOE must protect itself and	O.SELFPROTECT provides TOE self-protection mechanisms which

Assumptions	Objectives	Rationale
	its platform content from unauthorized access and tampering.	satisfy this assumption.
A.TIMESTAMP The IT environment provides the TOE with the necessary reliable timestamps.	OE.TIME The TOE environment must provide reliable timestamps to the TOE.	OE.TIME satisfies the assumption that the environment provides reliable timestamps to the TOE.

Every assumption is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives uphold all defined assumptions.

8.3 Rationale for Extended Security Functional Requirements

There are no extended functional requirements defined for this TOE.

8.4 Rationale for Extended TOE Security Assurance Requirements

There are no extended assurance requirements defined for this TOE.

8.5 Security Requirements Rationale

The following discussion provides detailed evidence of coverage for each security objective.

8.5.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 15 - Objectives:SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges (and only those TOE users) may exercise such control.	FAU_GEN.1 Audit Data Generation	The requirement meets this objective by ensuring that the TOE provides the ability to manage the audit function, and that only authorized administrators are permitted to manage this function.
	FMT_MOF.1 Management of security functions behaviour	The requirement meets the objective by ensuring that the TOE restricts administrative functions to only those users with the appropriate privileges.
	FMT_MSA.1 Management of security attributes	The requirement meets the objective by ensuring that the TOE restricts the ability to manipulate security attributes to

Objective	Requirements Addressing the Objective	Rationale
		only those users with the appropriate privileges.
	FMT_MSA.3 Static attribute initialisation	The requirement meets the objective by ensuring that the TOE creates restrictive default values for security attributes.
	FMT_MTD.1 Management of TSF data	The requirement meets the objective by ensuring that the TOE restricts access to TSF data based on the administrator's privileges.
	FMT_SMF.1 Specification of management functions	The requirement meets the objective by ensuring that the TOE includes administrative functions to facilitate the management of the TSF.
	FMT_SMR.1 Security roles	The requirement meets the objective by ensuring that the TOE associates users with roles to provide access to TSF management functions and data.
O.AUDIT The TOE must record events of security relevance at the "not specified level" of audit. The TOE must record the resulting actions of the security functional policies and provide the authorized administrators with the ability to review the audit trail, and allow filtering to easily find information to aid in an investigation of a security violation.	FAU_GEN.1 Audit Data Generation	The requirement meets this objective by ensuring that the TOE maintains a record of defined security related events, including relevant details about the events.
	FAU_GEN.2 User identity association	The requirement meets this objective by ensuring that the TOE associates each auditable even with the identity of the user that caused the event.
	FAU_SAR.1 Audit review	The requirement meets the objective by ensuring that the TOE provides the ability to review logs.
	FAU_SAR.2 Restricted audit review	The requirement meets this objective by ensuring that the TOE allows the audit records to be read only by authorized users.
	FAU_SAR.3 Selectable audit review	The requirement meets this objective by ensuring that the TOE allows users to apply administrator-defined methods of searching, sorting, ordering, and filtering to the audit data based on administrator-defined criteria.

Objective	Requirements Addressing the Objective	Rationale
O.AUTHENTICATE The TOE must identify and authenticate users prior to allowing access to TOE administrative functions and data. The TOE must only allow authorized users to access appropriate TOE functions and data.	FDP_ACC.1 Subset access control	The requirement meets the objective by ensuring that access control is applied to all user operations.
	FDP_ACF.1 Security attribute based access control	The requirement meets the objective by ensuring that access control is applied to all user operations.
	FIA_UAU.2 User authentication before any action	The requirement meets the objective by ensuring that users are authenticated before access to TOE functions is allowed.
	FIA_UID.2 User identification before any action	The requirement meets the objective by ensuring that the users are identified before access to TOE functions is allowed.
	FMT_MOF.1 Management of security functions behaviour	The requirement meets the objective by ensuring that the TOE authenticates users prior to allowing access to administrative functions to ensure that only appropriately privileged users may manage the security behaviour of the TOE.
	FMT_MSA.1 Management of security attributes	The requirement meets the objective by ensuring that the TOE authenticates users prior to allowing security attributes to be manipulated, to ensure that only appropriately privileged users may do so.
	FMT_MSA.3 Static attribute initialisation	The requirement meets the objective by ensuring that the TOE authenticates users prior to allowing security attributes to be manipulated, to ensure that only appropriately privileged users may do so.
	FMT_MTD.1 Management of TSF data	The requirement meets the objective by ensuring that only authorized administrators are allowed access to manipulate security attributes and applications.
O.ACCESS The TOE must present the user with a security disclaimer prior to	FTA_TAB.1 TOE access banner	The requirement meets this objective by providing individuals with a security warning implying

Objective	Requirements Addressing the Objective	Rationale
identification and authentication to the TOE.		that unauthorized access is prohibited.
O.SELFPROTECT The TOE must protect itself and its platform content from unauthorized access and tampering.	FIA_AFL.1 Authentication failure handling	The requirement meets this objective by automatically locking user accounts after a number of unsuccessful authentication attempts.
	FTA_SSL.3 TSF-initiated termination	The requirement meets this objective by automatically terminating user sessions after a period of inactivity.

8.5.2 Security Assurance Requirements Rationale

EAL2++ was chosen to provide a moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor, assuming that the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. The TOE is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL2++, the TOE will have incurred a search for obvious flaws to support its introduction into the non-hostile environment.

The augmentation of ALC_FLR.2 was chosen to give greater assurance of the developer's on-going flaw remediation processes.

8.5.3 Dependency Rationale

This ST does satisfy all the requirement dependencies of the Common Criteria. Table 16 lists each requirement to which the TOE claims conformance with a dependency and indicates whether the dependent requirement was included. As the table indicates, all dependencies have been met.

Table 16 - Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	The TOE environment provides the timestamps for the TOE.
FAU_GEN.2	FAU_GEN.1	✓	
	FIA_UID.2	✓	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1 is included. This satisfies this dependency.
FAU_SAR.1	FAU_GEN.1	✓	
FAU_SAR.2	FAU_SAR.1	✓	

SFR ID	Dependencies	Dependency Met	Rationale
FAU_SAR.3	FAU_SAR.1	✓	
FDP_ACC.1	FDP_ACF.1	✓	
FDP_ACF.1	FMT_MSA.3	✓	
	FDP_ACC.1	✓	
FIA_UAU.2	FIA_UID.1	✓	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1 is included. This satisfies this dependency.
FIA_UID.2	No dependencies	✓	
FIA_AFL.1	FIA_UAU.1	✓	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1 is included. This satisfies this dependency.
FMT_MOF.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.1	FDP_ACC.1	✓	
	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.3	FMT_MSA.1	✓	
	FMT_SMR.1	✓	
FMT_MTD.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_SMF.1	No dependencies	✓	
FMT_SMR.1	FIA_UID.1	✓	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1 is included. This satisfies this dependency.
FTA_TAB.1	No dependencies.	✓	
FTA_SSL.3	No dependencies.	✓	

9 Acronyms

This section provides the acronyms used in this document.

Table 17 - Acronyms

Acronym	Definition
API	Application Programming Interface
CC	Common Criteria
CM	Configuration Management
EAL	Evaluation Assurance Level
eGRC	Enterprise Governance, Risk, and Compliance
IIS	Internet Information Services
IP	Internet Protocol
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
OS	Operating System
OSP	Organizational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Functional Policy
SFR	Security Functional Requirement
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality

Prepared by:
Corsec Security, Inc.

13135 Lee Jackson Memorial Highway
Suite 220
Fairfax, VA 22033
United States of America

Phone: +1 (703) 267-6050
Email: info@corsec.com
http://www.corsec.com