RSA Archer Suite v6.5
Security Target

Version 0.3
18 February 2019

Prepared for:

13200 Metcalf Avenue, Suite 300
Overland Park, KS 66213

Prepared By:

Accredited Testing and Evaluation Labs
6841 Benjamin Franklin Drive
Columbia, MD 21046

TABLE OF CONTENTS

LIST OF TABLES

1. Introduction

This section introduces the Target of Evaluation (TOE) and provides the Security Target (ST) and TOE identification, ST and TOE conformance claims, ST conventions, glossary and list of abbreviations.

The TOE is RSA Archer Suite v6.5. It comprises software that supports business-level management of governance, risk management, and compliance (GRC). It enables organizations to build an efficient, collaborative enterprise GRC program across IT, finance, operations and legal domains. It supports organizations in managing risk, demonstrating compliance, automating business processes, and gaining visibility into corporate risk and security controls.

The ST contains the following additional sections:

- TOE Description (Section 2)—provides an overview of the TOE and describes the physical and logical boundaries of the TOE
- Security Problem Definition (Section 3)—describes the threats and assumptions that define the security problem to be addressed by the TOE and its environment
- Security Objectives (Section 4)—describes the security objectives for the TOE and its operational environment necessary to counter the threats and satisfy the assumptions that define the security problem
- IT Security Requirements (Section 5)—specifies the security functional requirements (SFRs) and security assurance requirements (SARs) to be met by the TOE
- TOE Summary Specification (Section 6)—describes the security functions of the TOE and how they satisfy the SFRs
- Rationale (Section 7)—provides mappings and rationale for the security problem definition, security objectives, security requirements, and security functions to justify their completeness, consistency, and suitability.

1.1 Security Target, TOE and CC Identification

ST Title – RSA Archer Suite v6.5 Security Target

ST Version – Version 0.3

ST Date – 18 February 2019

TOE Identification – RSA Archer Suite v6.5

TOE Developer – RSA

Evaluation Sponsor – RSA

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017

1.2 Conformance Claims

This ST and the TOE it describes are conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components, Version 3.1 Revision 5, April 2017.
    - Part 2 Conformant
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, Version 3.1 Revision 5, April 2017.
    - Part 3 Conformant

This ST and the TOE it describes are conformant to the following package:

- EAL2 Augmented (ALC_FLR.2).

1.3 Conventions

The following conventions are used in this document:

- Security Functional Requirements—Part 1 of the CC defines the approved set of operations that may be applied to functional requirements: iteration; assignment; selection; and refinement.
    - Iteration—allows a component to be used more than once with varying operations. In this ST, iteration is identified with a number in parentheses following the base component identifier. For example, iterations of FCS_COP.1 are identified in a manner similar to FCS_COP.1(1) (for the component) and FCS_COP.1.1(1) (for the elements).
    - Assignment—allows the specification of an identified parameter. Assignments are indicated using bold text and are enclosed by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [***[selected-assignment]***]).
    - Selection—allows the specification of one or more elements from a list. Selections are indicated using bold italics and are enclosed by brackets (e.g., [***selection***]).
    - Refinement—allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
- Other sections of the ST—other sections of the ST use bolding to highlight text of special interest, such as captions.

1.4 Glossary

This ST uses a number of terms that have a specific meaning within the context of the ST and the TOE. This glossary provides a list of those terms and how they are to be understood within this ST.

Access Role	A collection of application-level and page-level rights that an administrator can create and assign to any number of users and groups to control user privileges (create, read, update, and delete).
Advanced Workflow	A feature of RSA Archer Suite that supports the management of the lifecycle of records representing ongoing business processes in applications or questionnaires.
Application	Contains specific types of data records, such as incidents, controls, policies or assets. The application defines the content and behavior of the individual records.
Dashboard	A container for one or more iViews, typically for the purpose of grouping related content. An administrator builds global dashboards that enable the user to create personal dashboards. If user permissions allow, the user can display global dashboards. The user cannot display the personal dashboards of other users.
Field	A container for a specific piece of data within a record. Different field types collect different of types of data, such as text, dates, or images. Each field has a configurable set of properties that govern how the field displays in the application and how (or whether) the user interacts with it.
iView	A window that is embedded in a workspace used to display a report, a chart, links to internal pages and external websites, an embedded web page, and custom content such as a Flash presentation or graphic.
Questionnaire	A questionnaire is structurally similar to an application but with attributes that support risk assessment processes. A questionnaire is tied to a target application to facilitate the assessment of specific target objects.

Record	An individual entry within an application or questionnaire. A record contains fields, which can be arranged in multiple sections.
Solution	A grouping of applications or questionnaires that work together to address a particular business need.
Sub-form	A grouping of fields that can be embedded in any application to collect information in individual records. When users add or edit a record in an application that contains a sub-form, they can add data to the sub-form multiple times.
Workspace	A page within the TOE GUI that contains one or more dashboards, which are accessible from a tab in the workspace tab strip. If a workspace has more than one dashboard, the user can select a dashboard from the Dashboard list in the page toolbar.

1.5 Abbreviations and Acronyms

This following abbreviations and acronyms are used throughout this ST:

API	Application Programming Interface
CC	Common Criteria
EAL	Evaluation Assurance Level
ETW	Event Tracing for Windows
GRC	Governance, Risk and Compliance
GUI	Graphical User Interface
IIS	Microsoft Internet Information Service
JRE	Java Runtime Environment
LDAP	Lightweight Directory Access Protocol
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

2. TOE Description

2.1 TOE Overview

Governance, Risk and Compliance (GRC) represents a business oriented approach to establishing ownership and accountability throughout an organization to improve decision making.

Governance is the act of directing, controlling and evaluating the culture, policies, processes, laws, and institutions that define the structure by which organizations are directed and managed.

Risk is the negative effect of uncertainty on achieving objectives, while Risk Management is the coordination of activities to direct and control an organization to realize opportunities while managing negative events.

Compliance is the act of adhering to, and demonstrating adherence to, external laws and regulations as well as organizational policies and procedures.

RSA Archer Suite v6.5 is a software product that supports business-level management of governance, risk management, and compliance. As the foundation for all RSA Archer Suite Solutions, the Suite allows users to adapt the solutions to their requirements, build their own applications, and integrate with other systems without touching code.

A *solution* is a grouping of related applications and questionnaires that address a particular business need. *Applications* and *questionnaires* are both containers for specific types of data records, such as incidents, controls, policies or assets. The application defines the content and behavior of the individual records. Questionnaires are structurally similar to applications but have unique features that allow users to assess the content of a particular target application. A *record* is an individual entry within an application or questionnaire. A record contains fields, which are often arranged in multiple sections. A *field* is a container for a specific piece of data within a record. Different field types collect different of types of data, such as text, dates, or images. Sensitive data can be stored encrypted in the database.

Users access the TOE via a web-based graphical user interface (GUI). All users require an account in order to log on to the TOE. The user account specifies the user's groups and access roles. An access role is a collection of application-level and page-level rights that an administrator can create and assign to any number of users and groups to control user privileges (create, read, update, and delete). The TOE controls user access to its objects (applications, questionnaires, records and fields) based on the access roles associated with users and with the groups to which the user belongs. An administrator can configure an advanced workflow to require users to electronically sign records. The electronic signature provides an additional layer of security by requiring users to re-authenticate before interacting with the records.

The Content API, Web Services API and RESTful APIs programmatically extend the functionality of the TOE to external applications through several classes and methods which expose many of its features, allowing for a high level of integration with other products. All users must be successfully identified and authenticated by the TOE before gaining access to any other TOE services.

The TOE provides capabilities to configure minimum strength requirements (e.g., minimum length, required character sets) for passwords. The TOE can be configured to track the number of consecutive failed authentication attempts and block further authentication attempts for a configurable time period when the configured threshold has been met. The TOE will terminate interactive sessions that have been idle for a configurable period of time.

The TOE is able to generate audit records of security-relevant events occurring on the TOE and provides administrators with the ability to review audit records stored in the audit trail.

The TOE can be configured and operated in accordance with FIPS 140-2 requirements. The evaluated configuration can be operated in either the FIPS mode or non-FIPS mode.

2.2 TOE Architecture

2.2.1 TOE Components

There are four main components to an RSA Archer Suite installation:

- Web Application—the RSA Archer Suite application that runs on a web server. This application requires Microsoft Internet Information Service (IIS) and Microsoft .NET Framework 4.6.1 or 4.6.2.
- Services—the services complement the Web application and include the following:
    - RSA Archer Suite Cache—supports the caching solution for reducing the number of calls to the database by storing metadata, which consists of language, application, solution, and values list data. This service requires Java 8.
    - RSA Archer Suite Configuration—stores the configuration parameters of the RSA Archer Suite and RSA Archer Suite services. This service must be installed and enabled on all web and services servers.
    - RSA Archer Suite Instrumentation—supports message logging through Event Tracing for Windows (ETW) to a database. This service only needs to be active if ETW is being used.
    - RSA Archer Suite LDAP Synchronization—supports user and group maintenance by synchronizing the users and groups in RSA Archer Suite to users and groups in another system through Lightweight Directory Access Protocol (LDAP). This service only needs to be active if LDAP is being used to manage user accounts.
    - RSA Archer Suite Job Engine—administers all asynchronous job processing for RSA Archer Suite, such as data feeds, findings generation, notifications, recalculations, and system jobs. This service is vital to RSA Archer Suite and is required.
    - RSA Archer Suite Queueing—builds and maintains indexes for keyword search and file attachments. This service is required. Only one RSA Archer Suite Queuing service can be enabled for an RSA Archer Suite instance. Support is provided for optional independent licensing of Elasticsearch for keyword and global searches for faster and more efficient indexing of content when large record volumes are present. The Elasticsearch capability is outside the TOE boundary.
    - RSA Archer Suite Workflow—administers the Advanced Workflow feature for processing workflows. This service is an integral part of RSA Archer Suite and should be running all the time. For solutions in which the Advanced Workflow feature is available, workflow does not function unless the RSA Archer Suite Workflow service is running.
- Instance Database—stores the RSA Archer Suite content for a specific instance. There can be multiple instances based on the business structure and product licensing. For example, there might be individual instances for each office location or region or for development, test, and production environments.
- Configuration Database—a central repository for configuration information for the web application and services servers.

In addition to the Web Application, Services, and Instance Database components, the RSA Archer Suite distribution includes the RSA Archer Suite Control Panel, a configuration tool used to create and manage RSA Archer Suite instances. The control panel enables RSA Archer Suite administrators to manage installation settings, instance settings, and plugins, but is not itself part of RSA Archer Suite and is outside the TOE boundary.

2.2.2 Deployment Architecture

The TOE can be deployed in single and multi-server configurations, depending on business requirements.

For optimal scalability and performance, RSA recommends a multi-server configuration. This configuration includes dedicated servers for hosting the web application and the services. Each server plays a specific role within the TOE configuration.

Although not recommended, the TOE can also be installed in a basic configuration consisting of a single server that hosts the web application and services.

Regardless if the TOE is deployed in a single or multi-server configuration, the database are installed on a dedicated server known as the database server.

2.2.3 TOE Physical Boundaries

The hardware requirements in the operational environment are determined by the size of the deployment and are summarized in the table below.

Size	Content Records	Concurrent Users	Description	Element
Very Small Single-Host Environment	Up to 75,000	Up to 10	Web, Services, and Database Servers all on the same server.	2 CPU Cores 8 GB RAM
Small Environment	Up to 100,000	Up to 100	Combined Web and Services Server with a separate Database Server.	For all servers: 4 CPU Cores 16 GB RAM
Medium Environment	Up to 250,000	Up to 250	Two Web Servers, one for Advanced Workflow and one for Web Application, one Services Server, and one Database Server.	For Web and Services Servers: 4 CPU Cores 16 GB RAM For Database Servers: 8 CPU Cores 48 GB RAM
Large Environment	Up to 750,000	Up to 750	Four Web Servers, two Services Servers with Advanced Workflow, and one Database Server.	For Web and Services Servers: 8 CPU Cores 24 GB RAM For Database Servers: 16 CPU Cores 96 GB RAM
Very Large Environment	More than 750,000	More than 750	Contact your RSA sales representative for very large environment recommendations.	
Offline Access Laptop	Up to 1,000	1	Standalone computer that can manual sync with RSA Archer for offline use.	2 CPU Cores 6 GB RAM

Table 1: Hardware Requirements

The TOE comprises the software and database components listed in Section 2.2.1 above.

The Web Application requires the following components in its operational environment:

- Windows Server 2012 R2 or 2016 Standard or Datacenter edition
- Internet Information Services Version 8.5 or 10 (included in Windows Server 2012 R2 or 2016)

- Microsoft Office 2010 or 2013 Filter Packs (to enable indexing of MS Office files). This in turn requires Microsoft Filter Pack 2.0 or later
- Microsoft .NET Framework 4.6.1 or 4.6.2

The Services component requires the following in its operational environment:

- Windows Server 2012 R2 or 2016 Standard or Datacenter edition
- Java Runtime Environment (JRE) 8
- Microsoft .NET Framework 4.6.1 or 4.6.2
- Microsoft Sync Framework 2.1 (for offline access).

The Instance and Configuration databases require the following in the operational environment:

- Windows Server 2012 R2 or 2016 Standard or Datacenter edition
- Microsoft SQL Server 2016 SP 1 (64-bit), Microsoft SQL Server 2016 Enterprise Edition or Microsoft SQL Server 2017 (64-bit).

Users accessing the TOE from a client computer require:

- One of the following supported browsers:
    - Internet Explorer 11
    - Internet Explorer Edge*
    - Chrome 69*
    - Firefox 62 or 60 (ESR)*
    - Safari 11*

  * These browsers do not support RSA Archer Administrator pages that require Silverlight.
- Microsoft Silverlight 5.1 (required for administration.)

The TOE must be configured to require the use of HTTPS to access the TOE from external clients. The TOE documentation provides the guidance necessary to configure the TOE in this fashion.

The following diagram is a representation of the physical boundaries of the TOE and its components.

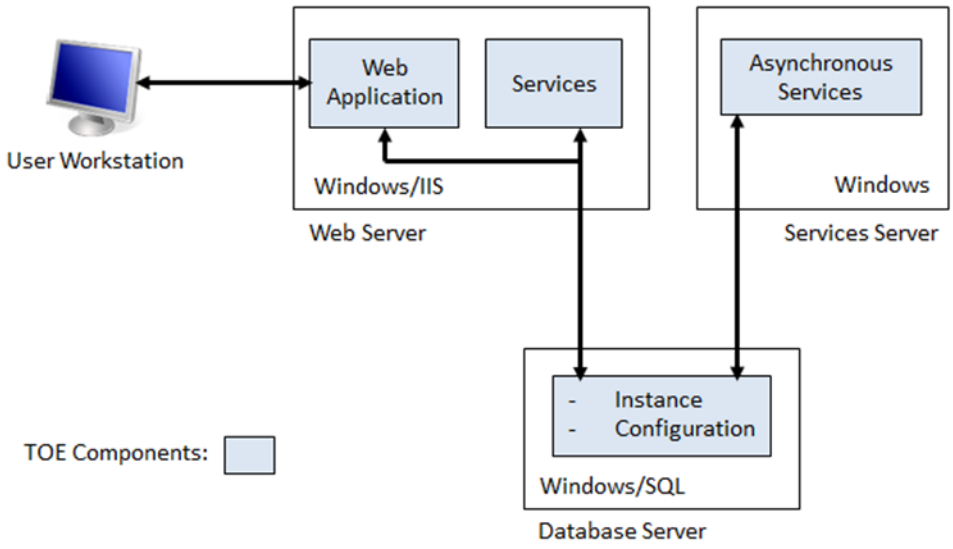

Figure 1: TOE Physical Boundaries

2.2.4 TOE Logical Boundaries

This section summarizes the security functions provided by the TOE.

2.2.4.1 Security Audit

The TOE generates audit records of security relevant events that include at least the date and time of the event, subject identity and outcome for security events. The TOE provides authorized administrators with the ability to read the audit events.

The TOE relies on its operational environment to store the audit records and to provide the system clock information that is used by the TOE to timestamp each audit record.

2.2.4.2 User Data Protection

The TOE implements a Discretionary Access Control security function policy (SFP) to control access by authorized users to the resources it manages. The scope of the Discretionary Access Control SFP covers applications, questionnaires, sub-forms, records, fields, workspaces, dashboards, and iViews.

2.2.4.3 Identification & Authentication

The TOE identifies and authenticates all users of the TOE before granting them access to the TOE. Each user must have an account on the TOE in order to access the TOE. The account associates the user's identity with the user's password, any assigned groups, and any assigned access roles. The TOE enforces minimum requirements for the construction of user passwords and provides a mechanism to lock a user account after a configured number of consecutive failed attempts to logon.

2.2.4.4 Security Management

Authorized administrators manage the security functions and TSF data of the TOE via the web-based GUI.

2.2.4.5 TOE Access

The TOE will terminate interactive sessions after a period of inactivity configurable by an administrator. The TOE also allows user-initiated termination of the user's own interactive session by explicitly logging off.

The TOE displays a banner message on the user login page. The content of the message is specified during initial configuration using the RSA Archer Suite Control Panel.

The TOE can be configured to allow connections to the Web Application only from designated IP addresses, and to deny session establishment outside specified times, days of the week, or dates.

2.3 TOE Documentation

This section identifies the guidance documentation included in the TOE, as follows:

- RSA Archer Platform Release Notes 6.5, October 2018
- RSA Archer Suite What's New Guide 6.5, October 2018
- RSA Archer Suite Qualified and Supported Environments 6.5, October 2018
- RSA Archer Suite Security Configuration Guide 6.5, October 2018
- RSA Archer Suite Platform Planning Guide 6.5, October 2018
- RSA Archer Suite Platform Installation and Upgrade Guide 6.5, October 2018
- RSA Archer Suite Content API Reference Guide 6.5, October 2018
- RSA Archer Suite RESTful API Reference Guide 6.5, October 2018
- RSA Archer Suite Web Services API Reference Guide 6.5, October 2018
- RSA Archer Suite What's New Guide 6.5, October 2018
- RSA Archer Suite Control Panel Guide 6.5, October 2018
- RSA Archer Suite Platform Administrator's Guide 6.5, October 2018

- RSA Archer Suite Platform User's Guide 6.5, October 2018

3. Security Problem Definition

This section defines the security problem to be addressed by the TOE, in terms of threats to be countered by the TOE or its operational environment, and assumptions about the intended operational environment of the TOE.

3.1 Assumptions

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

A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.PROTECT	The TOE software critical to security policy enforcement will be protected from unauthorized physical modification.
A.SECURE_COMMS	The operational environment of the TOE will provide mechanisms to protect data communicated to and from remote users from disclosure and modification.
A.TIME	The operational environment of the TOE will provide reliable time sources for use by the TOE.
A.CRYPTO	The TOE will use cryptographic primitives provided by the Operational Environment to perform cryptographic services.

3.2 Threats

This section identifies and describes the threats to be countered by the TOE and its operational environment.

T.BRUTE_FORCE	An unauthorized user may gain access to the TOE through repeated password-guessing attempts.
T.DATA_COMPROMISE	Authorized users of the TOE perform unauthorized actions on the objects controlled by the TOE.
T.INAPPROPRIATE_USE	Authorized users perform inappropriate actions on the TOE due to ignorance of their responsibilities or operational policies and procedures, or access the TOE at unapproved times or from unapproved locations.
T.NO_ACCOUNTABILITY	Authorized users of the TOE perform adverse actions on the TOE, or attempt to perform unauthorized actions, which go undetected.
T.UNATTENDED_SESSION	An unauthorized user gains access to the TOE via an unattended authorized user session.
T.UNAUTHORIZED_ACCESS	An unauthorized user may gain access to the TOE security functions and data.
T.UNAUTHORIZED_ACTIVITY	Authorized users perform unauthorized actions on the TOE.

4. Security Objectives

This section identifies the security objectives for the TOE and its operational environment. The security objectives identify the responsibilities of the TOE and its environment in addressing the security problem defined in Section 3.

4.1 Security Objectives for the TOE

The following are the TOE security objectives:

O.ACCESS_CONTROL	The TOE shall enforce an access control policy to restrict the operations authorized users can perform on objects controlled by the TOE.
O.AUDIT	The TOE shall be able to generate audit records of security-relevant events, identifying users causing the events as applicable.
O.AUDIT_REVIEW	The TOE shall provide a means for authorized users to review the audit records generated by the TOE.
O.I_AND_A	The TOE shall require all users of the TOE to be identified and authenticated before gaining access to TOE services.
O.LOGON_BANNER	The TOE shall be able to display a configurable advisory warning message to potential users pertaining to appropriate use of the TOE.
O.PASSWORD_CONTROLS	The TOE shall provide a mechanism to reduce the likelihood that users choose weak passwords.
O.SECURITY_MANAGEMENT	The TOE shall restrict the ability to perform security management functions on the TOE to authorized administrators having appropriate privileges.
O.SESSION_LIMITATION	The TOE shall provide a mechanism to place constraints on the ability of an authorized user to establish a session with the TOE.
O.SESSION_TERMINATION	The TOE shall provide mechanisms to terminate a user session after a period of inactivity or at the request of the user.
O.THROTTLE	The TOE shall limit the rate at which consecutive unsuccessful authentication attempts can be performed.

4.2 Security Objectives for the Operational Environment

The following are the security objectives for the operational environment of the TOE.

OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
OE.PERSONNEL	Those responsible for the TOE must ensure that personnel working as authorized administrators have been carefully selected and trained for proper operation of the TOE.
OE.SECURE_COMMS	The operational environment provides mechanisms to protect all data communicated to and from remote users from disclosure and modification.
OE.TIME	The operational environment provides reliable time sources for use by the TOE.
OE.CRYPTO	The Operational Environment will provide cryptographic primitives that can be used by the TOE to provide services such as ensuring the confidentiality of sensitive data stored in the database.

5. IT Security Requirements

5.1 TOE Security Functional Requirements

This section specifies the security functional requirements (SFRs) for the TOE. SFRs were drawn exclusively from Part 2 of the Common Criteria v3.1 Revision 5.

Requirement Class	Requirement Component
FAU: 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
FDP: User Data Protection	FDP_ACC.1: Subset access control
	FDP_ACF.1: Security attribute based access control
FIA: Identification and Authentication	FIA_AFL.1: Authentication failure handling
	FIA_ATD.1: User attribute definition
	FIA_SOS.1: Verification of secrets
	FIA_UAU.2: User authentication before any action
	FIA_UAU.6: Re-authenticating
	FIA_UID.2: User identification before any action
FMT: 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_REV.1: Revocation
	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.1: Security roles
FTA: TOE Access	FTA_SSL.3: TSF-initiated termination
	FTA_SSL.4: User-initiated termination
	FTA_TAB.1: Default TOE access banners
	FTA_TSE.1: TOE session establishment

Table 2: TOE Security Functional Components

5.1.1 Security Audit (FAU)

FAU_GEN.1 – Audit data generation

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

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

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

c) [**The following auditable events:**
- **Access role created, modified, deleted**
- **Account status modified**
- **Application owner added, deleted**
- **Sub-form owner added, deleted**
- **Full application content deleted**
- **Global report permission granted, removed**
- **LDAP configuration delete, started, completed**
- **Offline access sync requested – download, upload**
- **User login succeeded, failed**
- **User logout**
- **Maximum login retries exceeded**
- **User account added, modified, deleted**
- **User added to group, removed from group**
- **User login name modified**
- **User full name modified**
- **Password changed by administrator**
- **Password changed by user**
- **Password reset requested**
- **Role assigned to user, removed from user**
- **Security parameter created, modified, deleted**
- **Security parameter assignment modified.**].

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, [**none**].

FAU_GEN.2 – User identity association

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.

FAU_SAR.1 – Audit review

FAU_SAR.1.1 The TSF shall provide [**System Administrator, User with Access Control rights**] with the capability to read [**all audit information**] from the audit records.

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

FAU_SAR.2 – Restricted audit review

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.

FAU_SAR.3 – Selectable audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply [**filtering**] of audit data based on [**event type or date range**].

5.1.2 User Data Protection (FDP)

FDP_ACC.1 – Subset access control

FDP_ACC.1.1 The TSF shall enforce the [**Discretionary Access Control SFP**] on [
- **Subjects: Users**

- **Objects: Applications, Questionnaires, Sub-forms, Records, Fields, Workspaces, Dashboards, iViews**
- **Operations:**
  - **Applications, Questionnaires, Sub-forms: access**
  - **Records: create, read, update, delete**
  - **Fields: read, edit**
  - **Workspaces, Dashboards, iViews, Effective Permissions Investigation Console: access**].

FDP_ACF.1 – Security attribute based access control

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

- **Subject Attributes:**
  - **User Name**
  - **Group**
  - **Access Role**
- **Object Attributes:**
  - **Application, Questionnaire, Sub-form: owner**
  - **Effective Permissions Investigation Console, Record: permissions**
  - **Field: permissions (Public, Private)**
  - **Workspace, Dashboard, iView: access (Public, Private)].**

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

- **Application, Questionnaire, Sub-form:**
  - **If an Application, Questionnaire, or Sub-form has no owners assigned, it can be accessed only by a User with the System Administrator access role.**
- **Record:**
  - **A User can create, read, update or delete a Record if the User or a Group of which the User is a member is granted the appropriate permission by the Application, Questionnaire or Sub-form containing the Record.**
- **Field:**
  - **A User can read a Field with Private permissions if the User or a Group of which the User is a member is granted Read-only or Full Access to the Field**
  - **A User can edit a Field with Private permissions if the User or a Group of which the User is a member is granted Full Access to the Field**
- **Workspace, Dashboard, iView:**
  - **A User can access a Workspace, Dashboard, or iView with Private permissions if the User or a Group of which the User is a member is assigned to the Workspace, Dashboard, or iView.**
- **Effective Permissions Investigation Console:**
  - **A User can access the Effective Permissions Investigation Console if the user is a System Administrator or a user granted appropriate permissions].**

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [

- **Application, Questionnaire:**
  - **A User who is assigned as an owner of an Application or Questionnaire, or is a member of a group that is assigned as an owner of an Application or Questionnaire, has unrestricted access to the Application or Questionnaire**
- **Field:**
  - **All Users have full access to a Field with Public permissions (subject to record-level permissions or data-driven events, which may hide or disable a field)**
- **Workspace, Dashboard, iView:**
  - **All Users have full access to a Workspace, Dashboard, or iView with Public permissions**].

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

5.1.3 Identification and authentication (FIA)

FIA_AFL.1 – Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when [***[an administrator configurable positive integer within [1 and 99]]***] unsuccessful authentication attempts occur related to [**user account login**].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [***met***], the TSF shall [**lock the user account associated with the failed authentication attempts for an administrator configurable period of time**].

FIA_ATD.1 – User attribute definition

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

- **User Name**
- **Password**
- **Group membership**
- **Access role**
- **Security parameters**].

FIA_SOS.1 – Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [**the following default requirements for all user accounts (except sysadmin and service accounts):**

- **Passwords must have a minimum length of 9 characters**
- **Passwords must contain at least 2 alphabetic characters**
- **Passwords must contain at least 1 uppercase character**
- **Passwords must contain at least 1 lowercase character**
- **Passwords must contain at least 1 numeric character**
- **Passwords must contain at least 1 special character**].

FIA_UAU.2 – User authentication before any action

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.

FIA_UAU.6 – Re-authenticating

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions [**interactive user session duration exceeds configured Static Session Timeout value, electronically sign records**].

FIA_UID.2 – User identification before any action

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.

5.1.4 Security Management (FMT)

FMT_MOF.1 – Management of security functions behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to [***disable, enable***] the functions [**data privacy**] to [**System Administrator**].

FMT_MSA.1 – Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [**Discretionary Access Control SFP**] to restrict the ability to [***query***, ***modify***, ***delete***] the security attributes [**Application, Questionnaire, or Sub-form owner; Record permissions; Field permissions; Workspace, Dashboard and iView access**] to [

- **an Application, Questionnaire, or Sub-form owner as appropriate (for Application, Questionnaire, or Sub-form owner; Record permissions; and Field permissions)**
- **Application Builder administrator, Workspace and Dashboard administrator (for Workspace, Dashboard and iView access)**
- **System Administrator (all security attributes)**].

FMT_MSA.3 – Static attribute initialisation

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

FMT_MSA.3.2 The TSF shall allow the [**Application, Questionnaire, and Sub-form owner; Application Builder administrator; Workspace and Dashboard administrator; System Administrator**] to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1(1) – Management of TSF data (user accounts, user groups)

FMT_MTD.1.1(1) The TSF shall restrict the ability to [***query, modify, delete, [create]***] the [**user accounts, user groups**] to [**System Administrator, User with Access Control rights**].

FMT_MTD.1(2) – Management of TSF data (access roles, security parameters)

FMT_MTD.1.1(2) The TSF shall restrict the ability to [***change_default, query, modify, delete, [create]***] the [**access roles, security parameters**] to [**System Administrator, User with Access Control rights**].

FMT_REV.1 – Revocation

FMT_REV.1.1 The TSF shall restrict the ability to revoke [**access roles**] associated with the [***users***] under the control of the TSF to [**System Administrator, User with Access Control rights**].

FMT_REV.1.2 The TSF shall enforce the rules [**immediately**].

FMT_SMF.1 – Specification of Management Functions

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

- **Manage user accounts**
- **Manage user groups**
- **Manage access roles**
- **Manage security parameters**
- **Manage data privacy**
- **Manage security attributes of objects within scope of Discretionary Access Control SFP**].

FMT_SMR.1 – Security roles

FMT_SMR.1.1 The TSF shall maintain the roles: [

- **System Administrator**
- **Application, Questionnaire, and Sub-form owner**
- **Application Builder administrator**
- **Workspace and Dashboard administrator**
- **User with Access Control rights**].

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

5.1.5 TOE Access (FTA)

FTA_SSL.3 – TSF-initiated termination

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [**time interval of user inactivity configured by System Administrator or User with Access Control rights**].

FTA_SSL.4 – User-initiated termination

FTA_SSL.4.1 The TSF shall allow user-initiated termination of the user's own interactive session.

FTA_TAB.1 – Default TOE access banners

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

FTA_TSE.1 – TOE session establishment

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on [**IP address, time of day, day of week, calendar date**].

5.2 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the EAL 2 augmented with ALC_FLR.2 components as specified in Part 3 of the Common Criteria. No operations are applied to the assurance components.

Requirement Class	Requirement Component
ADV: Development	ADV_ARC.1: Security architecture description
	ADV_FSP.2: Security-enforcing functional specification
	ADV_TDS.1: Basic design
AGD: Guidance documents	AGD_OPE.1: Operational user guidance
	AGD_PRE.1: Preparative procedures
ALC: Life-cycle support	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: 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
ATE: Tests	ATE_COV.1: Evidence of coverage
	ATE_FUN.1: Functional testing
	ATE_IND.2: Independent testing – sample
AVA: Vulnerability assessment	AVA_VAN.2: Vulnerability analysis

Table 3: TOE Security Assurance Components

5.2.1 Development (ADV)

ADV_ARC.1 – Security architecture description

ADV_ARC.1.1D The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.

ADV_ARC.1.3D The developer shall provide a security architecture description of the TSF.

ADV_ARC.1.1C The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

ADV_ARC.1.2C	The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.
ADV_ARC.1.3C	The security architecture description shall describe how the TSF initialisation process is secure.
ADV_ARC.1.4C	The security architecture description shall demonstrate that the TSF protects itself from tampering.
ADV_ARC.1.5C	The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.
ADV_ARC.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.2 – Security-enforcing functional specification

ADV_FSP.2.1D	The developer shall provide a functional specification.
ADV_FSP.2.2D	The developer shall provide a tracing from the functional specification to the SFRs.
ADV_FSP.2.1C	The functional specification shall completely represent the TSF.
ADV_FSP.2.2C	The functional specification shall describe the purpose and method of use for all TSFI.
ADV_FSP.2.3C	The functional specification shall identify and describe all parameters associated with each TSFI.
ADV_FSP.2.4C	For each SFR-enforcing TSFI, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.
ADV_FSP.2.5C	For each SFR-enforcing TSFI, the functional specification shall describe direct error messages resulting from processing associated with the SFR-enforcing actions.
ADV_FSP.2.6C	The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.
ADV_FSP.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_FSP.2.2E	The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

ADV_TDS.1 – Basic design

ADV_TDS.1.1D	The developer shall provide the design of the TOE.
ADV_TDS.1.2D	The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.
ADV_TDS.1.1C	The design shall describe the structure of the TOE in terms of subsystems.
ADV_TDS.1.2C	The design shall identify all subsystems of the TSF.
ADV_TDS.1.3C	The design shall provide the behaviour summary of each SFR-supporting or SFR-non-interfering TSF subsystem.
ADV_TDS.1.4C	The design shall summarise the SFR-enforcing behavior of the SFR-enforcing subsystems.
ADV_TDS.1.5C	The design shall provide a description of the interactions among SFR-enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.
ADV_TDS.1.6C	The mapping shall demonstrate that all TSFIs trace to the behavior described in the TOE design that they invoke.
ADV_TDS.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_TDS.1.2E	The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

5.2.2 Guidance Documents (AGD)

AGD_OPE.1 – Operational user guidance

AGD_OPE.1.1D	The developer shall provide operational user guidance.

AGD_OPE.1.1C	The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.
AGD_OPE.1.2C	The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.
AGD_OPE.1.3C	The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.
AGD_OPE.1.4C	The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.
AGD_OPE.1.5C	The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.
AGD_OPE.1.6C	The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.
AGD_OPE.1.7C	The operational user guidance shall be clear and reasonable.
AGD_OPE.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1 – Preparative procedures

AGD_PRE.1.1D	The developer shall provide the TOE including its preparative procedures.
AGD_PRE.1.1C	The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.
AGD_PRE.1.2C	The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.
AGD_PRE.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AGD_PRE.1.2E	The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

5.2.3 Life-cycle Support (ALC)

ALC_CMC.2 – Use of a CM system

ALC_CMC.2.1D	The developer shall provide the TOE and a reference for the TOE.
ALC_CMC.2.2D	The developer shall provide the CM documentation.
ALC_CMC.2.3D	The developer shall use a CM system.
ALC_CMC.2.1C	The TOE shall be labelled with its unique reference.
ALC_CMC.2.2C	The CM documentation shall describe the method used to uniquely identify the configuration items.
ALC_CMC.2.3C	The CM system shall uniquely identify all configuration items.
ALC_CMC.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_CMS.2 – Parts of the TOE CM coverage

ALC_CMS.2.1D	The developer shall provide a configuration list for the TOE.
ALC_CMS.2.1C	The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; and the parts that comprise the TOE.

ALC_CMS.2.2C	The configuration list shall uniquely identify the configuration items.
ALC_CMS.2.3C	For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.
ALC_CMS.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DEL.1 – Delivery procedures

ALC_DEL.1.1D	The developer shall document and provide procedures for delivery of the TOE or parts of it to the consumer.
ALC_DEL.1.2D	The developer shall use the delivery procedures.
ALC_DEL.1.1C	The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.
ALC_DEL.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_FLR.2 – Flaw reporting procedures

ALC_FLR.2.1D	The developer shall document and provide flaw remediation procedures addressed to TOE developers.
ALC_FLR.2.2D	The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.
ALC_FLR.2.3D	The developer shall provide flaw remediation guidance addressed to TOE users.
ALC_FLR.2.1C	The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.
ALC_FLR.2.2C	The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.
ALC_FLR.2.3C	The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.
ALC_FLR.2.4C	The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.
ALC_FLR.2.5C	The flaw remediation procedures shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.
ALC_FLR.2.6C	The procedures for processing reported security flaws shall ensure that any reported flaws are remediated and the remediation procedures issued to TOE users.
ALC_FLR.2.7C	The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.
ALC_FLR.2.8C	The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.
ALC_FLR.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4 Security Target Evaluation (ASE)

ASE_CCL.1 – Conformance claims

ASE_CCL.1.1D	The developer shall provide a conformance claim.
ASE_CCL.1.2D	The developer shall provide a conformance claim rationale.
ASE_CCL.1.1C	The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.
ASE_CCL.1.2C	The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.

ASE_CCL.1.3C	The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.
ASE_CCL.1.4C	The CC conformance claim shall be consistent with the extended components definition.
ASE_CCL.1.5C	The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.
ASE_CCL.1.6C	The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.
ASE_CCL.1.7C	The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.
ASE_CCL.1.8C	The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.
ASE_CCL.1.9C	The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.
ASE_CCL.1.10C	The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.
ASE_CCL.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_ECD.1 – Extended components definition

ASE_ECD.1.1D	The developer shall provide a statement of security requirements.
ASE_ECD.1.2D	The developer shall provide an extended components definition.
ASE_ECD.1.1C	The statement of security requirements shall identify all extended security requirements.
ASE_ECD.1.2C	The extended components definition shall define an extended component for each extended security requirement.
ASE_ECD.1.3C	The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.
ASE_ECD.1.4C	The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.
ASE_ECD.1.5C	The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.
ASE_ECD.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ASE_ECD.1.2E	The evaluator shall confirm that no extended component can be clearly expressed using existing components.

ASE_INT.1 – ST introduction

ASE_INT.1.1D	The developer shall provide an ST introduction.
ASE_INT.1.1C	The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.
ASE_INT.1.2C	The ST reference shall uniquely identify the ST.
ASE_INT.1.3C	The TOE reference shall uniquely identify the TOE.
ASE_INT.1.4C	The TOE overview shall summarise the usage and major security features of the TOE.
ASE_INT.1.5C	The TOE overview shall identify the TOE type.
ASE_INT.1.6C	The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.
ASE_INT.1.7C	The TOE description shall describe the physical scope of the TOE.

ASE_INT.1.8C	The TOE description shall describe the logical scope of the TOE.
ASE_INT.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ASE_INT.1.2E	The evaluator shall confirm that the TOE reference, the TOE overview, and the TOE description are consistent with each other.

ASE_OBJ.2 – Security objectives

ASE_OBJ.2.1D	The developer shall provide a statement of security objectives.
ASE_OBJ.2.2D	The developer shall provide a security objectives rationale.
ASE_OBJ.2.1C	The statement of security objectives shall describe the security objectives for the TOE and the security objectives for the operational environment.
ASE_OBJ.2.2C	The security objectives rationale shall trace each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective.
ASE_OBJ.2.3C	The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.
ASE_OBJ.2.4C	The security objectives rationale shall demonstrate that the security objectives counter all threats.
ASE_OBJ.2.5C	The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.
ASE_OBJ.2.6C	The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.
ASE_OBJ.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_REQ.2 – Derived security requirements

ASE_REQ.2.1D	The developer shall provide a statement of security requirements.
ASE_REQ.2.2D	The developer shall provide a security requirements rationale.
ASE_REQ.2.1C	The statement of security requirements shall describe the SFRs and the SARs.
ASE_REQ.2.2C	All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.
ASE_REQ.2.3C	The statement of security requirements shall identify all operations on the security requirements.
ASE_REQ.2.4C	All operations shall be performed correctly.
ASE_REQ.2.5C	Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.
ASE_REQ.2.6C	The security requirements rationale shall trace each SFR back to the security objectives for the TOE.
ASE_REQ.2.7C	The security requirements rationale shall demonstrate that the SFRs meet all security objectives for the TOE.
ASE_REQ.2.8C	The security requirements rationale shall explain why the SARs were chosen.
ASE_REQ.2.9C	The statement of security requirements shall be internally consistent.
ASE_REQ.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_SPD.1 – Security problem definition

ASE_SPD.1.1D	The developer shall provide a security problem definition.
ASE_SPD.1.1C	The security problem definition shall describe the threats.
ASE_SPD.1.2C	All threats shall be described in terms of a threat agent, an asset, and an adverse action.
ASE_SPD.1.3C	The security problem definition shall describe the OSPs.

ASE_SPD.1.4C	The security problem definition shall describe the assumptions about the operational environment of the TOE.
ASE_SPD.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_TSS.1 – TOE summary specification

ASE_TSS.1.1D	The developer shall provide a TOE summary specification.
ASE_TSS.1.1C	The TOE summary specification shall describe how the TOE meets each SFR.
ASE_TSS.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ASE_TSS.1.2E	The evaluator shall confirm that the TOE summary specification is consistent with the TOE overview and the TOE description.

5.2.5 Tests (ATE)

ATE_COV.1 – Evidence of coverage

ATE_COV.1.1D	The developer shall provide evidence of the test coverage.
ATE_COV.1.1C	The evidence of the test coverage shall show the correspondence between the tests in the test documentation and the TSFIs in the functional specification.
ATE_COV.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_FUN.1 – Functional testing

ATE_FUN.1.1D	The developer shall test the TSF and document the results.
ATE_FUN.1.2D	The developer shall provide test documentation.
ATE_FUN.1.1C	The test documentation shall consist of test plans, expected test results and actual test results.
ATE_FUN.1.2C	The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.
ATE_FUN.1.3C	The expected test results shall show the anticipated outputs from a successful execution of the tests.
ATE_FUN.1.4C	The actual test results shall be consistent with the expected test results.
ATE_FUN.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2 – Independent testing – sample

ATE_IND.2.1D	The developer shall provide the TOE for testing.
ATE_IND.2.1C	The TOE shall be suitable for testing.
ATE_IND.2.2C	The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.
ATE_IND.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ATE_IND.2.2E	The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.
ATE_IND.2.3E	The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

5.2.6 Vulnerability Assessment (AVA)

AVA_VAN.2 – Vulnerability analysis

AVA_VAN.2.1D	The developer shall provide the TOE for testing.
AVA_VAN.2.1C	The TOE shall be suitable for testing.

AVA_VAN.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.2.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.2.3E The evaluator shall perform an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design and security architecture description to identify potential vulnerabilities in the TOE.

AVA_VAN.2.4E The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

6. TOE Summary Specification

This section describes the following security functions implemented by the TOE to satisfy the SFRs claimed in Section 5.1:

- Security audit
- User data protection
- Identification and authentication
- Security management
- TOE access.

6.1 Security Audit

The TOE generates audit records (termed "security events" in the TOE documentation) for the following auditable events:

- Start-up and shutdown of the audit function (Security Events started/stopped)
- Access role created, modified, deleted
- Account status modified
- Application owner added, deleted
- Sub-form owner added, deleted
- Full application content deleted
- Global report permission granted, removed
- LDAP configuration delete, started, completed
- Offline access sync requested – download, upload
- User login succeeded, failed
- User logout
- Maximum login retries exceeded
- User account added, modified, deleted
- User added to group, removed from group
- User login name modified
- User full name modified
- Password changed by administrator
- Password changed by user
- Password reset requested
- Role assigned to user, removed from user
- Security parameter created, modified, deleted
- Security parameter assignment modified.

The audit records are written to the Security Events Report, which is a persistent report stored in the instance database. Each audit record includes the date and time of the security event, the type of security event, the subject identity, and the outcome (success or failure) of the event.

Users with the System Administrator access role or Access Control rights are able to view the contents of the Security Events Report via the Access Control menu of the TOE GUI. Only users with the System Administrator access role or Access Control rights are able to view the Security Events Report. The TOE provides the capability to filter the Security Events Report by event type or date range.

The TOE relies on its operational environment to provide secure storage of the audit trail in the instance database and to provide reliable time stamps in order to be able to record the date and time in generated audit records.

The Security Audit security function satisfies the following security functional requirements:

- FAU_GEN.1—audit records are generated for security relevant events and include the date and time of the event, type of event, subject identity, and outcome of the event.
- FAU_GEN.2—the TOE associates each auditable event resulting from actions of identified users with the identity of the user that caused the event.
- FAU_SAR.1—the TOE provides authorized users with the capability to read all audit information from the audit records. The audit records are displayed in a manner suitable for the authorized user to interpret the information.
- FAU_SAR.2—the TOE prohibits all users read access to the audit records, except those users that have been granted explicit read-access.
- FAU_SAR.3—the TOE provides capabilities to filter the audit data based on event type or date range.

6.2 User Data Protection

The TOE implements a Discretionary Access Control security function policy (SFP) to control access by authorized users to the resources it manages.

6.2.1 Controlled Objects

The TOE defines a number of objects that fall within the scope of control of the Discretionary Access Control SFP. The following paragraphs identify and describe these objects and the access controls or permissions that can be applied to them.

6.2.1.1 Applications

Applications contain specific types of data records, such as incidents, controls, policies, or assets. The TOE provides an Application Builder capability to define the properties of applications, such as the fields they contain, their layout, and their appearance in the Navigation Menu. Multiple applications can be grouped into solutions.

Each application has one or more owners, which can be users or groups. The creator of an application is automatically granted ownership rights to that application. Ownership rights can be revoked by other assigned owners.

6.2.1.2 Questionnaires

A questionnaire is structurally similar to an application but with unique qualities that enable administrators to better create and support risk assessment processes. A questionnaire is tied to a target application, such as Assets, Vendors, or Business Processes, to facilitate the assessment of specific target objects. Questionnaires include system-generated fields that calculate the progress, status, and scoring of individual questionnaire records. These system fields also enable administrators to assign submitters and reviewers for questionnaire records and to specify due dates.

As with applications, each questionnaire has one or more owners, which can be users or groups. The creator of a questionnaire is automatically granted ownership rights to that questionnaire. Ownership rights can be revoked by other assigned owners.

6.2.1.3 Sub-forms

A sub-form is a special grouping of fields that can be embedded in any application to collect information in individual records. When users add or edit a record in an application that contains a sub-form, they can add data to the sub-form multiple times.

Each sub-form has one or more owners, which can be users or groups. The creator of a sub-form is automatically granted ownership rights to that sub-form. Ownership rights can be revoked by other assigned owners. Sub-forms inherit record permissions from the application or questionnaire they are placed in.

6.2.1.4 Records

A record is an individual entry within an application or questionnaire. A record contains fields, which can be arranged in multiple sections.

User rights to records are granted at the application/questionnaire, record or field level, as follows:

- Application/Questionnaire—create, read, update, and delete permissions determine whether a user can add, edit, delete, and search records within an application or questionnaire
- Record—if an application or questionnaire contains a record permissions field, users can access only the fields to which they have permissions
- Field—individual fields in an application or questionnaire are either public or private (see sub-section 6.2.1.5 below for further details).

The record permissions field supports the following permission models for granting record-level access to users and groups:

- Automatic—record-level permissions are granted based on rules specifying data conditions within the record
- Manual—record-level permissions are granted by selecting users and groups in the field.
- Inherited—record-level permissions are inherited from related data levels or applications.

Automatic permissions model

In the Automatic permissions model, record-level permissions are granted based on rules specifying data conditions within the record. One or more rules are defined for assigning record access based on data conditions within the record. When a rule is created, one or more conditions for rule fulfillment are defined. A condition consists of a field to evaluate and one or more values to watch for in that field. After the conditions are defined, the users and groups who have access to records in which the specified conditions are met are selected. When the users and groups are selected, the permissions those users and groups have are specified—read-only access or update and delete access.

The Automatic permissions model also requires that one or more default users or groups are selected who have access to records in which none of the rules are met. The permissions default users and groups have (read-only access or update and delete access) are also specified.

Permissions are recalculated for individual records each time a value changes that causes a new rule to prove true.

Manual permissions model

In the Manual permissions model, record-level permissions are granted by selecting users and groups in the field. The application owner must select at least one user or group from which users can select. By default, all users and groups selected in a record permissions field have read access to their assigned records. Update and delete access can also be granted. Rules can also be defined to control the level of permissions the selected users and groups receive based on record content.

Inherited permissions model

In the Inherited permissions model, record permissions are inherited from related levels or applications. Permissions set in one record are automatically applied to related records. If a parent-level record with child-level records that inherit permissions from it is deleted, the permissions in the child-level records are also deleted. When this model is used, at least one Record Permissions field in a related application or data level must be selected from which to inherit permissions.

The TOE defines two mutually-exclusive rules specifying how permissions are inherited:

- Unrestricted—record permissions are inherited from all related records. When the permissions are set in a record, those permissions automatically apply to all related records.

Restricted—record permissions are inherited from selected related records. When the permissions are set in a record, those permissions automatically apply to the specified related records.

6.2.1.5 Fields

A field is a container for a specific piece of data within a record. Different field types collect different of types of data, such as text, dates, or images. Each field has a configurable set of properties that govern how the field displays in the application and how (or whether) the user interacts with it.

Each field has access rights or permissions associated with it that determine whether all users or only select users or groups have access to the field. Field permissions can be Public (the field is available to all users) or Private (available only to users and groups to which access rights are granted). Access rights can be: Full Access (read and edit); or Read-only. Access rights can be extended to sub-groups of a group granted access.

6.2.1.6 Workspaces, Dashboards, iViews

Each time an Application Builder administrator creates a new solution, a workspace is automatically created for that solution. The workspace shares the solution name, and access to the workspace is granted to the administrator who created the solution. Once a solution-based workspace is created, Workspace and Dashboard administrators can configure the workspace properties, including its content, Navigation Menu settings, and access rights.

Access rights can be assigned to iViews, dashboards, and workspaces. Access can be either Public (the iView, dashboard or workspace is available to all users) or Private (available only to users and groups to which access rights are granted).

6.2.2 Subject Security Attributes

The TOE defines the following user security attributes that are employed when making access control decisions within the scope of the Discretionary Access Control SFP:

- User Name—the identity associated with the user in the user's account
- Group—a means of grouping users based on some common criterion such as organizational structure or geographic location. Groups are hierarchical—a group can contain users or other groups of users.
- Access Role—a collection of application-level and page-level rights that control user privileges (create, read, update, and delete). Access roles can be assigned to users directly or through group membership. Access roles are cumulative and can be assigned to any number of users or groups, and users can have more than one access role. For example, one access role grants create, read, and update privileges in the Policies applications and another access role grants only delete privileges. A user who is assigned both access roles possesses create, read, update, and delete privileges in the Policies applications.

When a user attempts to access a controlled object, the TOE determines the access rights the user has to the object based on the access roles assigned to the user.

6.2.3 Access Control Rules

The TOE implements access control rules for each of the controlled objects within the scope of the Discretionary Access Control SFP, based on an object's owner or permissions attributes and on a user's name, group memberships, and access roles.

The owner of an application or questionnaire has unrestricted access to all record content in the application or questionnaire, including sub-form content. If no users have been assigned ownership, only users who have been granted the System Administrator access role can open an application or questionnaire for editing.

Sub-form owners can edit and customize sub-forms to which they are assigned, but owners do not automatically have access rights for the content stored in the sub-form. If no users have been assigned ownership, only users who have been granted the System Administrator or Manage Subforms access role can open a sub-form for editing.

A user can perform create, read, update or delete operations on a record if the user or a group of which the user is a member is granted the appropriate permission by the application or questionnaire containing the record.

If an application, questionnaire, or sub-form contains a record permissions field, a user can access only the fields for which they are granted permissions. Individual fields in an application or questionnaire are either public or private. Public fields are available to all users who have create, read, update, and delete permissions. Private fields are only available to selected users who can view and enter data in those fields. Private fields can also be "read only" for any user, which allows the user to view the field but not to add, edit, or delete its data.

A user can access a workspace, dashboard, or iView with Private permissions if the user, or a group of which the user is a member, is assigned to the Workspace, Dashboard, or iView. All users have full access to a workspace, dashboard, or iView with Public permissions.

The User Data Protection security function satisfies the following security functional requirements:

- FDP_ACC.1, FDP_ACF.1—the TOE implements the Discretionary Access Control SFP to control access of TOE users to RSA Archer Suite resources.
- FMT_MSA.1—the TOE restricts the ability to manage security attributes associated with applications, questionnaires, sub-forms, records and fields to application, questionnaire and sub-form owners as appropriate and to users in the System Administrator role. Additionally, the TOE restricts the ability to manage access rights associated with workspaces, dashboards and iViews to Application Builder administrators and Workspace and Dashboard administrators and to users in the System Administrator role.
- FMT_MSA.3—the TOE provides permissive default values for the security attributes associated with objects in the scope of the Discretionary Access Control SFP. The security management roles authorized to manage the security attributes associated with these objects are able to specify alternative initial values to override the default values when an object is created.

6.3 Identification and Authentication

Each TOE user must have an account to log on to the TOE.

6.3.1 Default User Accounts

The TOE defines a number of default user accounts—a System Administration account (**sysadmin**) and several services accounts. When a new instance of the TOE is created, the installer requires the user to enter a password for the **sysadmin** account and the service accounts. The service accounts are as follows:

- **userArcherAdvancedWorkFlowService**—service account for the Advanced Workflow service, which performs system interactions for tasks passing through workflow stages
- **userArcherAssetServer**—service account for the Asset service, which is an internal service used by the Web Application to retrieve shared resources
- **userArcherAsyncService**—service account for job management and the Indexing Service
- **userArcherCalculationAccount**—service account for calculations
- **userArcherDataFeedService**—service account for data feeds
- **userArcherLdapService**—service account for LDAP synchronization
- **userArcherNotificationService**—service account for notifications
- **userMigrationUser**—service account for migration
- **userOfflineService**—service account for Offline Access.

The **userMigrationUser** account can be used only by the installer, while each of the other service accounts can be used only by TOE services. Users cannot log on to any of these accounts, and none of these accounts can be renamed or deleted.

6.3.2 User Attributes

The TOE associates the following security attributes with each user account:

- User Name—the identity claimed by the user when logging in to the TOE. The User Name is a seven character system-defined name in all lowercase. The User Name contains the first six characters of the user's Last Name (as entered by the administrator) followed by the first character of the user's First Name (as entered by the administrator). If the Last Name is fewer than six characters, the system uses additional characters from the First Name to make a seven-character user name. If the user name is not unique in the domain, the system appends a number (up to 999) to the end of the name to make the name unique.
- Password—the authentication data associated with the account User Name.
- Security parameter—specifies password and authorization rules for the user account. The password rules determine the strength requirements for the user's password while the authorization rules determine how the user accesses their account.
- Groups—the user groups to which the user belongs.
- Access roles—access roles are cumulative and can be assigned to any number of users or groups, and users can have more than one access role.

6.3.3 Password Policy

The TOE enforces password strength, logon, and session time-out policies specified by security parameters defined in the Administration workspace. These parameters are enforced by the TOE across all user accounts, except for the **sysadmin** and service accounts. The following table identifies the security parameters associated with password strength and their default values.

Security Parameter	Default Value
Minimum password length	9 characters
Alpha characters required	2 characters
Numeric characters required	1 character
Special characters required	1 character
Uppercase characters required	1 character
Lowercase characters required	1 character

Table 4: Password Policy Parameters and Default Values

6.3.4 Logging On

The TOE requires users to provide identification, in the form of a user name, and authentication data, in the form of a password, in order to gain access to the TOE.

The TOE is able to detect when an administrator configurable positive integer of unsuccessful authentication attempts occur related to user authentication. When the defined number of unsuccessful authentication attempts has been met (the default is three), the TOE locks the user account for a specified time period as configured by the System Administrator or user with Access Control rights (the default is 999 days).

The number of consecutive failed login attempts allowed and the account lockout duration are maintained as authorization properties in the security parameters associated with the user's account. The System Administrator or user with Access Control rights can also configure the Static Session Timeout field in the authorization properties. A user is required to re-authenticate their interactive session if the duration of the session exceeds the Static Session Timeout value configured in the security parameters associated with the user's account.

An administrator can configure an advanced workflow to require signatures on user action nodes. The electronic signature provides an additional layer of security by requiring users to re-authenticate before interacting with the records. Administrators choose between two authentication processes:

- Password - This requires the user to enter their password to continue.
- Email Notification with PIN - This sends an email notification to the user's default email address. Users enter the PIN to continue.

The Identification and Authentication function satisfies the following security functional requirements:

- FIA_AFL.1—the TOE is able to detect when an administrator-configurable positive integer of unsuccessful authentication attempts occur related to user authentication. When the defined number of unsuccessful authentication attempts has been met, the TOE locks the user account for a specified time period as configured by authorized administrator.
- FIA_ATD.1—the TOE maintains the following security attributes associated with each user: Username; Password; Group Membership, Access Role, and Security Parameters.
- FIA_SOS.1—the TOE enforces a password policy that ensures all secrets (i.e., passwords) associated with user accounts meet policy requirements.
- FIA_UAU.2—the TOE requires each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
- FIA_UAU.6—the TOE requires a user to re-authenticate their interactive session if the duration of the session exceeds the configured Static Session Timeout value. An administrator configured advanced work flow requires users to re-authenticate on the user action nodes before interacting with the records.
- FIA_UID.2—the TOE requires each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.4 Security Management

6.4.1 Security Management Roles

The TOE uses its “access role” mechanism to define security management roles supported by the TOE. An access role is a collection of administrative, application-level and page-level rights that an administrator can create and assign to any number of users and groups to control user privileges (create, read, update, and delete). For example, the access role of a General User might allow access only to applications, while the access role of an Administrative User might allow access only to TOE security management features.

The TOE includes a pre-defined access role called System Administrator that cannot be modified or deleted. The System Administrator role grants users unrestricted access to all TOE features and to all records stored in applications. Only users who have already been designated as System Administrators can assign the System Administrator role to other users.

The pre-packaged solutions provided with the TOE also include pre-defined access roles for use within the solution.

Access roles are assigned to users through group membership or directly to user accounts. In the context of the SFRs defined in the ST, the TOE supports the following security management roles:

- System Administrator—has full access to all TOE features and all data on the TOE
- User with Access Control rights—has full access to the Access Control page of the GUI
- Application, Questionnaire, and Sub-form owner—has full access to the application, questionnaire or sub-form of which it is an owner
- Application Builder administrator—has full access to solution workspace for solutions the administrator has created
- Workspace and Dashboard administrator—has full access to workspaces, dashboards and iViews.

6.4.2 Security Management Functions

In the context of the SFRs defined in the ST, the TOE provides the following security management functions:

- Manage user accounts—the System Administrator and users with Access Control rights can create, query, modify and delete user accounts
- Manage user groups—the System Administrator and users with Access Control rights can create, query, modify and delete user groups
- Manage access roles—the System Administrator and users with Access Control rights can create, query, modify, change default and delete access roles
- Manage security parameters—the System Administrator and users with Access Control rights can create, query, modify, change default and delete security parameters
- Manage security attributes of objects within scope of Discretionary Access Control SFP—see Section 6.2 for descriptions of the capabilities and restrictions on management of security attributes of objects within scope of Discretionary Access Control SFP.
- Manage data privacy – the System Administrator can enable the date, IP address, numeric fields, text fields, new and existing Image and Attachment fields to be encrypted in an application. The encryption protects sensitive data stored in the database.

The Security Management function satisfies the following security functional requirements:

- FMT_MOF.1 - The TOE provides the capability to manage data privacy.
- FMT_MTD.1(*)—the TOE restricts the ability to manage the TSF data (user accounts, user groups, access roles, security parameters) to the System Administrator and users with Access Control rights.
- FMT_REV.1—the TOE provides the capability to immediately revoke access roles associated with user accounts.
- FMT_SMF.1—the TOE provides the capabilities necessary to manage the security of the TOE.
- FMT_SMR.1—the TOE defines security management roles based on the rights assigned to individual user accounts. The TOE additionally defines a built-in System Administrator role that has full access to all TOE features and all data on the TOE.

6.5 TOE Access

The TOE can be configured to terminate an interactive user session after a specified time interval of user inactivity. Users with the System Administrator access role or Access Control rights are able to configure the timeout value for an inactive session in the Authorization Properties section of Security Parameters.

The TOE allows user-initiated termination of the user's own interactive session by explicitly logging off.

The TOE defines a logon banner that displays a message at the bottom of the Login page (i.e., prior to users completing the identification and authentication process). By default, the message is blank. The RSA Archer Suite Control Panel is used to configure the message to be displayed.

Users with the System Administrator access role or Access Control rights are able to configure the following Authorization Properties that can be used to restrict user session establishment:

- Time period allowed for user sessions—when enabled, this property allows active user sessions only during a specific time period (e.g., 8:00am – 6:00 pm). The TOE will deny attempts to establish a session outside the specified time period
- Days disallowed for user sessions—this property specifies days of the week (e.g., Saturday, Sunday) when user sessions are disallowed. The TOE will deny attempts to establish a user session on the selected days
- Dates disallowed for user sessions—this property specifies calendar dates (e.g., 25 December) when user sessions are disallowed. The TOE will deny attempts to establish a user session on the specified dates.

In addition, the RSA Archer Suite Control Panel can be used to configure an IP Whitelist to specify the range of IP addresses that are allowed to connect to the designated RSA Archer Suite web server for all instances or only a

specific instance. Multiple IP addresses can be specified, either individually or as a range. The TOE will deny attempts to establish a user session originating from an IP address not specified in the IP Whitelist.

The TOE Access security function satisfies the following security functional requirements:

- FTA_SSL.3—the TOE terminates an interactive session after a time interval of user inactivity configured by an authorized administrator.
- FTA_SSL.4—the TOE allows user-initiated termination of the user's own interactive session.
- FTA_TAB.1—the TOE can be configured to display an advisory warning message regarding unauthorized use of the TOE.
- FTA_TSE.1—the TOE can be configured to deny session establishment based on IP address, time of day, days of week, and calendar dates.

7. Rationale

This section provides the rationale for completeness and consistency of the Security Target. The rationale addresses the following areas:

- Security Objectives
- Security Functional Requirements
- Security Assurance Requirements
- Requirement Dependencies
- TOE Summary Specification.

7.1 Security Objectives Rationale

This section shows that all secure usage assumptions and threats are completely covered by security objectives for the TOE or operational environment. In addition, each objective counters or addresses at least one assumption or threat.

	T.BRUTE_FORCE	T.DATA_COMPROMISE	T.INAPPROPRIATE_USE	T.NO_ACCOUNTABILITY	T.UNATTENDED_SESSION	T. UNAUTHORIZED_ACCESS	T.UNAUTHORIZED_ACTIVITY	A. MANAGE	A. PROTECT	A.SECURE_COMMS	A.TIME	A.CRYPTO
O.ACCESS_CONTROL		X										
O.AUDIT				X								
O.AUDIT_REVIEW				X								
O.I_AND_A						X						
O.LOGON_BANNER			X									
O.PASSWORD_CONTROLS	X											
O.SECURITY_MANAGEMENT							X					
O.SESSION_LIMITATION			X									
O.SESSION_TERMINATION					X							
O.THROTTLE	X											
OE.PHYSICAL									X			
OE.PERSONNEL								X				
OE.SECURE_COMMS										X		
OE.TIME											X	
OE.CRYPTO												X

Table 5: Security Problem Definition to Security Objective Correspondence

T.BRUTE_FORCE

An unauthorized user may gain access to the TOE through repeated password-guessing attempts.

This threat is countered by the following security objectives:

- O.PASSWORD_CONTROLS—addresses this threat by providing a mechanism, configurable by an administrator, which encourages users to choose difficult-to-guess passwords.

- O.THROTTLE—addresses this threat by providing a mechanism, configurable by an administrator, to lock a user account after a specified number of consecutive failed authentication attempts has been met.

T.DATA_COMPROMISE

Authorized users of the TOE perform unauthorized actions on the objects controlled by the TOE.

This threat is countered by the following security objective:

- O.ACCESS_CONTROL—addresses this threat by enforcing an access control policy that restricts the operations users can perform on the objects controlled by the TOE.

T.INAPPRORIATE_USE

Authorized users perform inappropriate actions on the TOE due to ignorance of their responsibilities or operational policies and procedures, or access the TOE at unapproved times or from unapproved locations.

This threat is countered by the following security objectives:

- O.LOGON_BANNER—addresses this threat by displaying a configurable advisory warning message to potential users pertaining to appropriate use of the TOE.
- O.SESSION_LIMITATION—addresses this threat by providing a mechanism to deny user session establishment based on such attributes as the time of day, day of the week, calendar date, or IP address.

T.NO_ACCOUNTABILITY

Authorized users of the TOE perform adverse actions on the TOE, or attempt to perform unauthorized actions, which go undetected.

This threat is countered by the following security objectives:

- O.AUDIT—addresses this threat by ensuring the TOE is able to generate audit records of security relevant events.
- O.AUDIT_REVIEW—supports O.AUDIT in addressing the threat by ensuring the TOE provides capabilities for effective review of stored audit records.

T.UNATTENDED_SESSION

An unauthorized user gains access to the TOE via an unattended authorized user session.

This threat is countered by the following security objective:

- O.SESSION_TERMINATION—addresses this threat by providing users with a mechanism to terminate their interactive sessions with the TOE, and by ensuring sessions that have been inactive for a configurable period of time will be terminated by the TOE.

T.UNAUTHORIZED_ACCESS

An unauthorized user may gain access to the TOE security functions and data.

This threat is countered by the following security objective:

- O.I_AND_A—addresses this threat by ensuring all users of the TOE are identified and authenticated prior to gaining further access to the TOE and its services.

T.UNAUTHORIZED_ACTIVITY

Authorized users perform unauthorized actions on the TOE.

This threat is countered by the following security objective:

O.SECURITY_MANAGEMENT—addresses this threat by providing a mechanism that requires authorized users to have appropriate privileges in order to perform actions on the TOE.

A.CRYPTO

The TOE will use cryptographic primitives provided by the Operational Environment to perform cryptographic services.

This assumption is satisfied by the following security objective:

- OE.CRYPTO The Operational Environment will provide cryptographic primitives that can be used by the TOE to provide services such as ensuring the confidentiality of sensitive data stored in the database.

A.MANAGE

There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

This assumption is satisfied by the following security objective:

- OE.PERSONNEL—this objective satisfies the assumption by ensuring those assigned as authorized administrators are properly trained in operating the TOE.

A.PROTECT

The TOE software critical to security policy enforcement will be protected from unauthorized physical modification..

This assumption is satisfied by the following security objective:

- OE.PHYSICAL—this objective satisfies the assumption by ensuring the TOE is protected from physical attack.

A.SECURE_COMMS

The operational environment of the TOE will provide mechanisms to protect data communicated to and from remote users from disclosure and modification.

This assumption is satisfied by the following security objective:

- OE.SECURE_COMMS—this objective satisfies the assumption by ensuring the operational environment provides mechanisms to protect transmitted data from disclosure and modification. The guidance documentation instructs the administrator to configure the TOE to use secure protocols (HTTPS) to protect communications between administrator clients and the TOE.

A.TIME

The operational environment of the TOE will provide reliable time sources for use by the TOE.

This assumption is satisfied by the following security objective:

- OE.TIME—this objective satisfies the assumption by ensuring the environment provides a reliable time source for use by the TOE. The underlying Windows operating system on which the TOE is installed provides a date/time function that is available for the TOE.

7.2 Security Functional Requirements Rationale

All security functional requirements identified in this Security Target are fully addressed in this section and each is mapped to the objective it is intended to satisfy. Table 6 summarizes the correspondence of functional requirements to TOE security objectives.

	O.ACCESS_CONTROL	O.AUDIT	O.AUDIT_REVIEW	O.I_AND_A	O.LOGON_BANNER	O.PASSWORD_CONTROLS	O.SECURITY_MANAGEMENT	O.SESSION_LIMITATION	O.SESSION_TERMINATION	O.THROTTLE
FAU_GEN.1		X								
FAU_GEN.2		X								
FAU_SAR.1			X							
FAU_SAR.2			X							
FAU_SAR.3			X							
FDP_ACC.1	X									
FDP_ACF.1	X									
FIA_AFL.1										X
FIA_ATD.1				X						
FIA_SOS.1						X				
FIA_UAU.2				X						
FIA_UAU.6				X						
FIA_UID.2				X						
FMT_MOF.1							X			
FMT_MSA.1	X									
FMT_MSA.3	X									
FMT_MTD.1(*)							X			
FMT_REV.1							X			
FMT_SMF.1							X			
FMT_SMR.1							X			
FTA_SSL.3									X	
FTA_SSL.4									X	
FTA_TAB.1					X					
FTA_TSE.1								X		

Table 6: Objectives to Requirement Correspondence

O.ACCESS_CONTROL

The TOE shall enforce an access control policy to restrict the operations authorized users can perform on objects controlled by the TOE.

The following security functional requirements contribute to satisfying this security objective:

- FDP_ACC.1, FDP_ACF.1—the ST includes FDP_ACC.1 and FDP_ACF.1 to specify the access control policy enforced by the TOE to control access to RSA Archer Suite objects by authorized RSA Archer Suite users.
- FMT_MSA.1, FMT_MSA.3—the ST includes FMT_MSA.1 and FMT_MSA.3 to specify restrictions on the management of security attributes used to control access to RSA Archer Suite objects

O.AUDIT

The TOE shall be able to generate audit records of security-relevant events, identifying users causing the events as applicable.

The following security functional requirements contribute to satisfying this security objective:

- FAU_GEN.1—the ST includes FAU_GEN.1 to specify the capability to generate audit records of security-relevant events, and to specify the specific events to be audited and the content of generated audit records of those events.
- FAU_GEN.2—the ST supports FAU_GEN.1 by including FAU_GEN.2 to specify the capability to include, when applicable, the identity of the user associated with the auditable event.

O.AUDIT_REVIEW

The TOE shall provide a means for authorized users to review the audit records generated by the TOE.

The following security functional requirements contribute to satisfying this security objective:

- FAU_SAR.1—the ST includes FAU_SAR.1 to specify which roles are to be able to read data from stored audit records.
- FAU_SAR.2—the ST supports FAU_SAR.1 by including FAU_SAR.2 to specify that the ability to read data from stored audit records is restricted to only the roles specified in FAU_GEN.1.
- FAU_SAR.3—the ST supports FAU_SAR.1 by including FAU_SAR.3 to specify capabilities for filtering audit records based on event type or date range, which assists the authorized roles in effectively reviewing the audit trail.

O.I_AND_A

The TOE shall require all users of the TOE to be identified and authenticated before gaining access to TOE services.

The following security functional requirements contribute to satisfying this security objective:

- FIA_UID.2, FIA_UAU.2—the ST includes FIA_UID.2 and FIA_UAU.2 to specify that users must be successfully identified and authenticated by the TOE before being able to perform any other TSF-mediated actions.
- FIA_UAU.6—the ST supports FIA_UAU.2 by including FIA_UAU.6 to ensure a user must re-authenticate to the TOE in the event their interactive session exceeds a configured time limit. An administrator configured advanced work flow requires users to re-authenticate on the user action nodes before interacting with the records.
- FIA_ATD.1—the ST supports FIA_UID.2 and FIA_UAU.2 by including FIA_ATD.1 to ensure user identity and authentication data security attributes are associated with individual users.

O.LOGON_BANNER

The TOE shall be able to display a configurable advisory warning message to potential users pertaining to appropriate use of the TOE.

The following security functional requirement contributes to satisfying this security objective:

- FTA_TAB.1—the ST includes FTA_TAB.1 to specify the capability to display an advisory warning message regarding unauthorized use of the TOE.

O.PASSWORD_CONTROLS

The TOE shall provide a mechanism to reduce the likelihood that users choose weak passwords.

The following security functional requirement contributes to satisfying this security objective:

- FIA_SOS.1—the ST includes FIA_SOS.1 to specify that passwords must meet minimum construction requirements, in terms of length and character set.

O.SECURITY_MANAGEMENT

The TOE shall restrict the ability to perform security management functions on the TOE to authorized administrators having appropriate privileges.

The following security functional requirements contribute to satisfying this security objective:

- FMT_SMF.1, FMT_MOF.1, FMT_SMR.1, FMT_MTD.1(*), FMT_REV.1—the ST includes these requirements to specify the security management functions to be provided by the TOE (FMT_SMF.1), to specify security management roles and privileges (FMT_SMR.1), to specify the restrictions on management of TSF data (FMT_MTD.1(*)), to manage data privacy (FMT_MOF.1), and to specify TOE behavior when security management privileges are revoked (FMT_REV.1).

O.SESSION_LIMITATION

The TOE shall provide a mechanism to place constraints on the ability of an authorized user to establish a session with the TOE.

The following security functional requirement contributes to satisfying this security objective:

- FTA_TSE.1—the ST includes FTA_TSE.1 to specify the capability for the TSF to deny session establishment based attributes such as time, day of week, date, and IP address.

O.SESSION_TERMINATION

The TOE shall provide mechanisms to terminate a user session after a period of inactivity or at the request of the user.

The following security functional requirements contribute to satisfying this security objective:

- FTA_SSL.3—the ST includes FTA_SSL.3 to specify the capability for the TSF to terminate an interactive user session after a period of inactivity.
- FTA_SSL.4—the ST includes FTA_SSL.4 to specify the capability for users to terminate their own interactive sessions.

O.THROTTLE

The TOE shall limit the rate at which consecutive unsuccessful authentication attempts can be performed.

The following security functional requirement contributes to satisfying this security objective:

- FIA_AFL.1—the ST includes FIA_AFL.1 to specify the capability to limit the rate at which consecutive failed authentication attempts (which may indicate a password-guessing attack) can be made.

7.3 Security Assurance Requirements Rationale

EAL 2 was selected as the assurance level because the TOE is a commercial product whose users require a low to moderate level of independently assured security. The TOE is targeted at an environment with good physical access security where it is assumed that attackers will have Basic attack potential. Augmentation was chosen to provide the added assurance that is gained by defining flaw remediation and flaw reporting procedures. Therefore, the target assurance level of EAL 2 augmented with ALC_FLR.2 is appropriate for such an environment.

7.4 Requirement Dependency Rationale

The following table identifies the SFRs claimed in the ST, their dependencies as defined in CC Part 2, and how the dependency is satisfied in the ST. It can be seen that all dependencies have been satisfied by inclusion in the ST of the appropriate dependent SFRs.

Requirement	Dependencies	How Satisfied
FAU_GEN.1	FPT_STM.1	See TimeStamp Note Below.
FAU_GEN.2	FAU_GEN.1, FIA_UID.1	FAU_GEN.1, FIA_UID.2 (hierarchical to

Requirement	Dependencies	How Satisfied
		FIA_UID.1)
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1, FMT_MSA.3
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2 (hierarchical to FIA_UAU.1)
FIA_ATD.1	None	None
FIA_SOS.1	None	None
FIA_UAU.2	FIA_UID.1	FIA_UID.2 (hierarchical to FIA_UID.1)
FIA_UID.2	None	None
FIA_UAU.6	None	None
FMT_MOF.1	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1, FMT_SMF.1	FDP_ACC.1, FMT_SMR.1, FMT_SMF.1
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1, FMT_SMR.1
FMT_MTD.1	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_REV.1	FMT_SMR.1	FMT_SMR.1
FMT_SMF.1	None	None
FMT_SMR.1	FIA_UID.1	FIA_UID.2 (hierarchical to FIA_UID.1)
FTA_SSL.3	None	None
FTA_SSL.4	None	None
FTA_TAB.1	None	None
FTE_TSE.1	None	None

Table 7: Requirement Dependencies

Timestamp Note: The TOE is not a physical device and operates as an application within a process provided by the environment. Thus, the environment is providing resources for the TOE. The environmental objective OE.TIME requires that the TOE's environment provide a reliable timestamp which the TOE can use as needed (e.g., within audit records). Thus, the functionality reflected in the dependency of FAU_GEN.1 upon FPT_STM.1 is available to the TOE from the environment.

7.5 TOE Summary Specification Rationale

Section 6, the TOE Summary Specification, describes how the security functions of the TOE meet the claimed SFRs. The following table provides a mapping of the SFRs to the security function descriptions to support the TOE Summary Specification.

	Security Audit	User Data Protection	Identification & Authentication	Security Management	TOE Access
FAU_GEN.1	X				
FAU_GEN.2	X				
FAU_SAR.1	X				

	Security Audit	User Data Protection	Identification & Authentication	Security Management	TOE Access
FAU_SAR.2	X				
FAU_SAR.3	X				
FDP_ACC.1		X			
FDP_ACF.1		X			
FIA_AFL.1			X		
FIA_ATD.1			X		
FIA_SOS.1			X		
FIA_UAU.2			X		
FIA_UAU.6			X		
FIA_UID.2			X		
FMT_MOF.1				X	
FMT_MSA.1		X			
FMT_MSA.3		X			
FMT_MTD.1				X	
FMT_REV.1				X	
FMT_SMF.1				X	
FMT_SMR.1				X	
FTA_SSL.3					X
FTA_SSL.4					X
FTA_TAB.1					X
FTA_TSE.1					X

Table 8: Security Functions vs. Requirements Mapping