



**MecWise HR 3.1 (R1)**  
**(MecWise eHuman Resource)**

# **Security Target**

Version 1.11  
Date: 4<sup>th</sup> September, 2010

## Document Information

This section describes the Security Target document history, briefly describes its intentions.

### Document History of Changes

No.	Version No.	Author	Version Date	Description of Changes
1	V1.11	Khairul Izhar Khalid Goo Kay Yaw Lim Beng Cheang	September 4 <sup>th</sup> , 2010	Final Revision

Table 1: Document History of Changes

### Contributors

- Khairul Izhar Khalid
- Lim Beng Cheang
- Goo Kay Yaw
- Members of the Core Development Team

## About Security Target Documentation

### What is Security Target?

- Implementation dependent statement of security needs for a specific identified Target of Evaluation (TOE)<sup>1</sup>

### How Security Target should be used

- The ST specifies “*what is to be evaluated*”. In this role, the ST serves as a basis for agreement between the developer and the evaluator on the exact security properties of the TOE and the exact scope of the evaluation. Technical correctness and completeness are major issues for this role. After the evaluation, the ST specifies “*what was evaluated*”. In this role, the ST serves as a basis for agreement between the developer or re-seller of the TOE and the potential consumer of the TOE. The ST describes the exact security properties of the TOE in an abstract manner, and the potential consumer can rely on this description because the TOE has been evaluated to meet the ST.<sup>2</sup>

<sup>1</sup> (Common Criteria Version 3.1 Revision 3 Part 1 - Introduction and General Model, 2009)

<sup>2</sup> (Common Criteria Version 3.1 Revision 3 Part 1 - Introduction and General Model, 2009)

### **Ingredients of Security Target Documentation (Common Criteria, 2009)**

The main contents of Security Target (ST) documentation is defined in the following constructs. (Please refer to the Table of Contents shown on the next page)

- Security Target Introduction (ASE\_INT) (Section 1)
  - Security Target Reference
  - Target of Evaluation Reference
  - Target of Evaluation Overview
  - Target of Evaluation Description
- Conformance Claims (ASE\_CCL) (Section 2)
  - Conformant to Common Criteria (CC) version,
  - Conformant to Common Criteria (CC) Part 2
  - Conformant to Common Criteria (CC Part 3
  - Protection Profile Conformance
  - Package Conformant (Evaluation Assurance Level (EAL))
- Security Objectives (ASE\_OBJ) (Section 3)
- Extended Components Definition (ASE\_ECD) (Section 4)
- Security Requirements (ASE\_REQ) (Section 5)
  - Security Functional Requirements
  - Security Assurance Requirements
  - Rationale for not addressing all dependencies
- Target of Evaluation Summary (ASE\_TSS) (Section 6)

## Table of Contents

Document Information.....	2
Table of Contents.....	4
List of Tables .....	5
List of Figures .....	6
Acronym List .....	7
1 Security Target (ST) Introduction.....	8
1.1 Security Target (ST) and Target of Evaluation Reference (TOE).....	8
1.2 Target of Evaluation (TOE) Overview .....	8
1.2.1 TOE Type.....	10
1.2.2 Hardware, Software and Firmware required by the TOE .....	10
1.3 Target of Evaluation (TOE) Description .....	12
1.3.1 Overview .....	12
1.3.2 Physical scope of the Target of Evaluation (TOE) .....	12
1.3.3 Logical scope of the Target of Evaluation (TOE) .....	13
2 Conformance Claim .....	15
3 Security Objectives .....	16
3.1 Security Objectives for the Operational Environment.....	16
4 Extended Components Definition.....	16
5 Security Requirements .....	18
5.1 Security Functionality Requirements.....	18
5.1.1 FAU Security Audit .....	18
5.1.2 FIA Identification and Authentication .....	19
5.1.3 FMT Security Management .....	19
5.1.4 FDP User Data Protection.....	21
5.2 Target of Evaluation (TOE) Security Assurance Requirement .....	22
5.3 Rationale for not addressing all dependencies.....	22
6 Target of Evaluation (TOE) Summary Specification .....	23
Figure 12: User account in displayed in User Account Profile. ....	32

## List of Tables

Table 1: Document History of Changes.....	2
Table 2: Acronym List .....	7
Table 3: Security Target (ST) & Target of Evaluation (TOE) Reference .....	8
Table 4: TOE security Modules and Functionalities Relationship .....	15
Table 5: Security Objectives for Operational Environment .....	16
Table 6: Extended Components .....	16
Table 7: FAU Security Audit.....	19
Table 8: FIA Identification and Authentication.....	19
Table 9: Security Management .....	21
Table 10: User Data Protection.....	21
Table 11: EAL1 (Evaluation Assurance Level 1) Class, Component IT and Component Title.....	22
Table 12: Logical TSF and Security Functional Requirements Mapping .....	23
Table 13: TSF Logical Scope - Audit Trail Utility and Security Functional Requirements Mapping .....	25
Table 14: TSF Logical Scope - Session Log Viewer and Security Functional Requirements Mapping.....	26
Table 15: TSF Logical Scope - Security Profile and Security Functional Requirements Mapping .....	26
Table 16: TSF Logical Scope - Security Group and Security Functional Requirements Mapping .....	31
Table 17: TSF Logical Scope - User Account Profile and Security Functional Requirements Mapping.....	33
Table 18: TSF Logical Scope – Web Interface and Security Functional Requirements Mapping .....	34

## List of Figures

Figure 1: Target of Evaluation (TOE) Logical Scope .....	13
Figure 2: Click on Audit Table Query table button to display Audit Trail data entries ...	24
Figure 3: Audit Table Query screen showing audit trail data.....	24
Figure 4: Module Access by Group Screen in Security Group .....	27
Figure 5: Screen of Security Group to list user that belongs to a group.....	27
Figure 6: Module Access screen showing Permission for EMPEFULL group on Pgrs% module.....	28
Figure 7: Create new Security Group, with no Module Access by Default .....	28
Figure 8: Security Access, Module Access by Group Screen with no permission selected by default. ....	29
Figure 9: Select and Delete permission were given to this group to act upon the selected module.....	29
Figure 10: List of Groups (roles) maintained in Security Group module.....	29
Figure 11: User tie to roles in Security Group module.....	30
Figure 12: User account in displayed in User Account Profile. ....	32

## Acronym List

No.	Acronym	Description (Definition)
1	CC	Common Criteria
2	EAL	Evaluation Assurance Level
3	ESS	Employee Self Service
4	HR	Human Resource
5	PP	Protection Profile
6	SAR	Security Assurance Requirements
7	SFR	Security Functional Requirements
8	ST	Security Target
9	TOE	Target of Evaluation
10	TSC	TSF Scope of Control
11	TSF	TOE Security Function
12	TSP	TOE Security Policy
13	TSS	TOE Summary Specification

Table 2: Acronym List

# 1 Security Target (ST) Introduction

This section describes the Target of Evaluation (TOE) in three levels of abstraction. This section consists of the following sub sections.

- Security Target (ST) and Target of Evaluation (TOE) References
- Target of Evaluation (TOE) Overview
- And Target of Evaluation (TOE) Description

## 1.1 Security Target (ST) and Target of Evaluation Reference (TOE)

1	<b>ST Title</b>	MecWise HR
2	<b>ST Version</b>	1.11
3	<b>ST Author</b>	StarVision Information Technology Sdn. Bhd.
4	<b>ST Publication Date</b>	September 4 <sup>th</sup> , 2010
5	<b>TOE Title</b>	MecWise HR
6	<b>TOE Version</b>	3.1 R1
7	<b>Evaluation Assurance Level (EAL)</b>	Assurance claims conform to EAL1 (Evaluation Assurance Level 1) from the Common Criteria for Information Technology Security Evaluation, Version 3.1.
8	<b>Keywords</b>	Security Profile, Security Group, User Account Profile, Audit Trail Utility, Session Transaction Log, Session Log Viewer

Table 3: Security Target (ST) & Target of Evaluation (TOE) Reference

## 1.2 Target of Evaluation (TOE) Overview

This section provides an overview to Target of Evaluation (TOE) and is targeted to potential consumers. The high level usage and security features of Target of Evaluation (TOE) are also highlighted.

- Also known as MecWise HR 3.1(R1) or MecWise eHuman Resource 3.1 (R1); the Target of Evaluation (TOE) is a web based Human Resource application or software that facilitates recording (entering), tracking, retrieving, reporting and maintaining of “*Employee Profile Information or data*”. The users of Target of Evaluation (TOE) are typically the management, administration or human resource personnel of an organization. The current version of TOE does not cater for employee self service (ESS) functionality.
- The Target of Evaluation (TOE) provides the following Human Resource related web interface modules to the authorized users (usually the HR users);
  - **Admin Masters:** Provision to create and managed company wide Human Resource related master file settings. The settings here will be use as



information input throughout other Human Resource modules and has no relation with the TOE security.

- **Personnel Masters:** Management of master file setup related to personnel events or data such as list of countries, list of nationalities, list of languages, will be use as selection input for employee profile setup (employee personal information), which is not related to the TOE security.
- **Employee Profile:** Provision to create, update and delete an employee profile, New appointment of employee into the company, Employee rejoin after leaving the company, and renumbering of employee's identity in HR system, which is not related to the employee's login identity of the system.
- **Position Database:** Management of Master data related to position and department of an organization, such as creation of new job family, creation of new department, and modification of department data. Information maintained here will serve as input for employee promotion and progress module.
- **Promotion and Progress:** Confirmation of an employee, Merits, upgrading and promotion
- **Leaving Service:** Termination of employment, Retirement and Resignation of employee.
- **Personnel Report:** Generation of HR Related Report in PDF and Excel Reports Format.

#### **TOE Security Overview:**

- The TOE Security comprises the following modules (Further explanation of the TOE security is described in the TOE description section 1.3);
  - **Security Profile** – Provides management and configuration of security related profiles.
  - **Security Group**– Enables creation and management of different security groups to which access rights to web interface modules can be assigned.
  - **User Account Profile** – Provides the creation and management of users' security attributes and profile.
  - **Session Log Viewer** – Enables the ability to view session logs of events
  - **Audit Trail Utility** – Provides the ability to enable/disable, view and filter transactions log events.
  - **Web interface** – Provides the ability to generate audit trail and session log records upon user performed actions.

The security functionalities provided by the TOE Security mentioned above are summarized as follows. The relationship between the functionalities described above and the TOE security is described in the Logical scope of the TOE Section 1.3.3 Table 4 TOE security Modules and Functionalities Relationship:

- **Audit Session Generation and Views** – provides the capability to generate user performed events through web interface. The session log events are triggered by Security Profile – Session Transaction Logs. The session log entry is accessible by authorized user (usually the Administrator of the TOE) via the Session Log Viewer. Audit Trail utility is also able to view and filter audit trail records.
- **Identification and Authentication** – provides the means for the authorize users to access the application. A username and password is required and it is matched against the record created by User Account Profile.
- **Security Management** - Enables the authorized administrator to create and manage User Account Profile, Security Group (e.g. module access) and Security Profile.

### 1.2.1 TOE Type

- The TOE type is a “Software”; (web based & utility application).

### 1.2.2 Hardware, Software and Firmware required by the TOE

The following highlights the Hardware, Software requirements by the TOE. It also describes the environment installation.

- **Hardware:**
  - TOE is a software application that requires a server (hardware). The basic hardware specification is a standard server with 1GHz or faster processor.
  - The TOE requires at least 1GB Memory or more.
  - The TOE requires a hard disk size space of 1GB or more (excluding the operating system and database software disk requirement space).
  - The TOE and the database (Microsoft SQL Server 2005) are to be installed on the same server hardware.
  - The TOE does not require any supporting appliances.
  - The TOE hardware is required to be connected in a network environment
- **Operating System:**
  - The TOE operates on Microsoft Windows 2003 Server operating system (32bit) (with Service Pack 2 installed).
- **Web Server software:**
  - The TOE requires an web Server; therefore Microsoft (Internet Information Server (IIS) Server version 6.0 is required to install on the server hardware
- **Database:**

- The TOE is dependent on Microsoft SQL Server 2005 database (with Service Pack 3 installed) as its repository.
- **Other Supporting software required by the TOE:**
  - Microsoft .NET Framework v2.0
  - Microsoft Windows Installer 3.1 by Default it is provided by Microsoft Windows 2003 Server.
  - Microsoft XML Core Services (MSXML) 4.0 Service Pack 3
  - Microsoft Data Access Components 2.8 (Service Pack 2)
  - SDA client installer V1.0 – External component provided by Third party to enable HR Report Generation to be provided together with the TOE during installation
  - A Web Browser known as Microsoft Internet Explorer 7

**Environment Installation Information:**

- The TOE is to be installed in a networked environment and without access to internet.
- The TOE does not require a fixed IP address (TCP/IP) and can be access based on the domain name or pc name. Client PC to access the TOE should be within the same Subnet as the server.
- Since the TOE is operating on a web based platform, to gain access to the TOE an authorized user requires at least a workstation/personal computer/notebook running on Microsoft Windows XP (with Service Pack 3 installed) and using an Microsoft Internet Explorer version 7 web browser client PC.

## 1.3 Target of Evaluation (TOE) Description

This section provides a narrative to TOE and is targeted to potential consumers and evaluators. The TOE includes both physical and logical scope (boundaries).

### 1.3.1 Overview

The TOE is software that provides web based human resource application. The TOE has Security Modules that comprises of the following

- Web Interface
- Security Profile
- Security Group
- User Account Profile
- Session Log Viewer
- and Audit Trail Utility

The TOE security modules mentioned above provides the identification and authentication, security management and also audit session generation and views functionalities. The relationship between the TOE security modules and its functionalities is explained in the logical scope of the target of evaluation (TOE) section 1.3.3.

### 1.3.2 Physical scope of the Target of Evaluation (TOE)

This sub section describes the physical scope of the TOE: a list of all hardware, firmware, software and guidance parts that constitute the Target of Evaluation (TOE).

The TOE **includes** the following

- MecWise HR 3.1 (R1) software;
- MecWise Audit Trail Utility software version 1.0 (file name: SC\_Audit.exe);

The TOE does not include:

- MecWise User License Manager Utility

#### **The Hardware/Firmware/Software Not Part of the TOE:**

The TOE **does not include** the following components:

- A Hardware Server;
- An Operating System on which the TOE is installed on;
- A Database Software on which the TOE is dependent on as its database;
- Microsoft Internet Information Services 6.0 Web Server;
- Other supporting software;
  - Microsoft .NET Framework Version 2.0

- Microsoft Windows Installer Version 3.1
- Microsoft XML Core Services (MSXML) Version 4.0
- Microsoft Data Access Components Version 2.8
- A Web Browser known as Microsoft Internet Explorer Version 7
- SDA Client Installer Version 1 – (Pre-requisite third party software to be distributed together with the TOE during installation of TOE).

### 1.3.3 Logical scope of the Target of Evaluation (TOE)

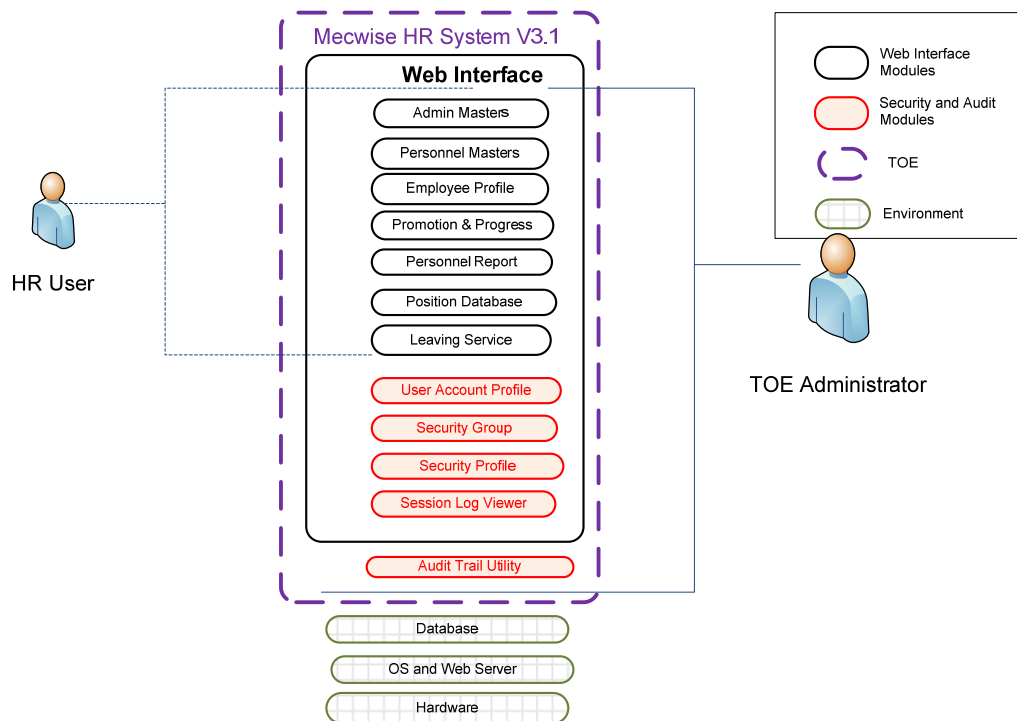


Figure 1: Target of Evaluation (TOE) Logical Scope

The diagram above describes the logical scope of the TOE. As mentioned in the overview Section 1.2 and Section 1.3.1, the TOE Security Module comprises of the following

- **Web Interface** – Provides the screens to access all parts of the TOE except Audit Trail Utility. Depends on the settings of Security Profile and Audit Trail Utility, actions that performed on the web interfaces such as Opening of Screen, Adding a New Record, Deletion of record or update of record will trigger the creation of the session log or audit trail records and will be recorded in a table accessible by Session Log Viewer or Audit Trail Utility.
- **Security Profile** – Enables management and configuration of security related profiles. The security profiles also enables the generation of “session transactions events” via the Session Transaction Log.

- **Security Group**– Enables creation and management of different security groups to which access rights to web interface modules can be assigned. Security group can also be referred as roles where the definition of module accessible by a single security group / role whether they have the ability to view, add, delete, modify record of a certain module which is user definable
- **User Account Profile** – Creation and Management of users’ security attributes such as user identification, password and password expiry control, controlling of modules accessible by a particular user in terms of security group joined.
- **Session Log Viewer** – Provide the ability to view session logs of events such as screen open, screen record Insertion, New Password, Screen Record Fetch, Screen Record Update and Screen Record Deletion.
- **Audit Trail Utility** - The event transactions pertaining to users’ activities related to a particular web interface module(s) which involve changed of data such as insert, modify, delete is stored in the audit log. Enable of Audit Trail feature is creation of an audit trail database table which have the similar structure of the original database table, and create a correspond database trigger on the tables. Within the audit trail utility, the authorized administrator will be able to view and filter audit trail records.

Based on the diagram, by default, TOE Administrator can access the modules in web interface modules of TOE, however TOE Administrator have the capability to determine to allow himself to access the web interface modules by including his own user identification in HR related security group.

For HR user to access the web interface modules, he or she needs to join under the respective Security Group (such as: HR Full) with Module access to the above Modules, with the exception of the set of security modules.

The following diagram describes the relationship of the TOE security modules with the functionalities defined earlier in section 1.3.1.

Functionalities	TOE Security Modules (based on the logical scope diagram)	Narrative
Identification and Authentication	User Account Profile	<p>User Identification such as username and password keyed in Login Page will be authenticated against the records created previously in <u>User Account Profile</u>.</p> <p>Provide the means to ensure that the authorized users are authenticated to the Target of Evaluation (TOE) via user</p>

Functionalities	TOE Security Modules (based on the logical scope diagram)	Narrative
		identification and password.
Security Management	Security Group Security Profile User Account Profile	<p>Enables the authorized administrator to manage security attributes such as user identification and password from the user account profile.</p> <p>The module access rights are managed from the Security Group.</p> <p>The selection of events to log is available at the Security Profile</p>
Audit Session Generation and Views	Security Profile – Session Transaction Log Audit Trail Utility Session Log Viewer Web interface	<p>Generation of Audit Trail record and session logs by web interface.</p> <p>Enables or disables the ability of the TOE to record Audit Trail records.</p> <p>The Security Profile – Session Transaction Log is intended for managing of events to be traced</p> <p>Both Audit Trail Utility and Session Log Viewer enable the authorized user to query and view the audit trail records.</p>

Table 4: TOE security Modules and Functionalities Relationship

## 2 Conformance Claim

The following conformance claims are made for the Target of Evaluation (TOE) and Security Target (ST):

- **Version of Common Criteria conformant.** The ST and the TOE are Common Criteria (CC) conformant to Common Criteria version 3.1 Revision 3.
- **Common Criteria Part 2 Extended.** The ST is Common Criteria (CC) Part 2 extended .
- **Common Criteria Part 3 conformant.** The ST is Common Criteria (CC) Part 3 conformant.
- **Package conformant.** The ST is package conformant to the package Evaluation Assurance Level EAL1
- **Protection Profile conformance.** No Protection Profile Claimed or Defined

## 3 Security Objectives

### 3.1 Security Objectives for the Operational Environment

No.	Reference Name	Description
1	OE_PHYSICAL	TOE must be installed in a physically secured location to prevent attacker from accessing the TOE physically
2	OE_RESPONSIBILITY	Person responsible of TOE must ensure TOE and any hardware/software/firmware required by TOE are delivered, installed, managed and operated in a secure manner.
3	OE_TOE_PASSWORD	That the TOE administrator and users must ensure that the password is hard to guess
4	OE_TOE_ADMIN	That the TOE administrator and users must ensure that the credentials of username and passwords are kept securely
5	OE_INTERNET	TOE must be operated without access to Internet

Table 5: Security Objectives for Operational Environment

## 4 Extended Components Definition

The following table contains the extended security functional requirements for the TOE:

Security Function Class	Security Function Components
FPT: Protection of TSF	FPT_STM_EXT.1 Reliable Time Stamps

Table 6: Extended Components



FPT class contains families of functional requirements that relate to the integrity and management of the mechanisms that constitute the TSF and to the integrity of TSF data. This component is a member of FPT\_STM, an existing CC Part 2 family. The following extended requirement for the FPT class has been included in this ST because the operational environment is capable of providing reliable time stamps for TSF functions, which is not covered in CC Part 2.

#### **FPT\_STM\_EXT.1 Reliable Time Stamps**

**Hierarchical to:** No other components.

**FPT\_STM\_EXT.1.1** The operational environment shall be able to provide reliable time stamps for TSF functions.

**Dependencies:** No dependencies.

**Application Note:** Reliable Time Stamps is required for the TOE to capture date and time events in relations to the FAU\_GEN.1 and FMT\_SAE.1 security functions. The TOE does not have feature to generate time stamps independently. However, the TOE is able to capture the date and time event from the environment which is derived from the Operating System

## 5 Security Requirements

This section contains the security functional requirements Security Functionality Requirement (SFR) for the Target of Evaluation (TOE). The Security Requirements consist of 2 groups; Security Functionality Requirements and Security Assurance Requirements. The Security Functionality Requirements is described in the sub sequent pages of section 5.

### 5.1 Security Functionality Requirements

The following conventions are set of operations that may be applied to functional requirements: assignment, selection, refinement and iteration.

- 1 The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by red **bold underline text**.
- 2 The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by red *italicized text* in square brackets, [*selection value*].
- 3 The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignment is indicated by showing the value in red square brackets, [**assignment value**].
- 4 The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing the iteration number in parenthesis following the component identifier, (iteration number).
- 5 The term “user” in general refers to a TOE User. In the TOE, a user’s role can be define by setting of the security group. A user with Security Module access is considered as TOE Administrator. Any user without security module access will then be treated as normal HR user. A administrator therefore will be able to alter all other users security group, which includes revoking other user’s access except his own account’s setting.

#### 5.1.1 FAU Security Audit

FAU_GEN.1 Audit Data Generation	
1. FAU_GEN.1.1	<p>The TSF shall be able to generate an audit record of the following auditable events:</p> <p>a) Start-up and shutdown of the audit functions <b><u>to be controlled by configuration of Security Profile and Audit Trail Utility</u></b>.</p> <p>b) All auditable events for the [<i>not specified</i>] level of audit; and</p> <p>c) [<b>Screen Open, Screen Fetch, Adding record, Deletion Record, Update Record, Login, Logout</b>].</p>
2. FAU_GEN.1.2	The TSF shall record within each audit record at least the

	<p>following information:</p> <p>a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and</p> <p>b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [Event related record data are recorded].</p>
<b>FAU_SAR.1 Audit Review</b>	
<b>3. FAU_SAR.1.1</b>	The TSF shall provide [administrator] with the capability to read [audit trail details, session log details] from the audit records.
<b>4. FAU_SAR.1.2</b>	The TSF shall provide the audit records in a manner suitable for the user to interpret the information.
<b>FAU_SEL.1 Selective Audit</b>	
<b>5. FAU_SEL.1.1</b>	<p>FAU_SEL.1.1 The TSF shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes:</p> <p>a) [event type]</p> <p>b) [table name]</p>

Table 7: FAU Security Audit

### 5.1.2 FIA Identification and Authentication

<b>FIA_ATD.1 User Attribute Definition</b>	
<b>6. FIA_ATD.1.1</b>	The TSF shall maintain the following list of security attributes belonging to individual users: [User Identity, Password, Employee ID, Security Profile, User Group, Data Access, Account Effective Date, Account Expiry Date, Password Expiry Date, Password history]

Table 8: FIA Identification and Authentication

### 5.1.3 FMT Security Management

<b>FMT_MOF.1 Management of Security Functions behaviour</b>	
<b>7. FMT_MOF.1.1</b>	The TSF shall restrict the ability to [ <i>determine the behaviour of, disable, enable, modify the behavior of</i> ] the functions [employee profile management, progression management, human resource reporting tools, master file maintenance, security] to [administrator].

<b>FMT_MSA.1 Management of Security Attributes</b>	
<b>8. FMT_MSA.1.1</b>	The TSF shall enforce the [access control SFP] to restrict the ability to [ <i>add, query, modify, delete, print</i> ] the security attributes [Security Group -module access] to [administrator] <b><u>which is user definable</u></b> .
<b>FMT_MSA.3 Static Attribute Initialization</b>	
<b>9. FMT_MSA.3.1</b>	The TSF shall enforce the [access control SFP – Security Group] to provide [ <i>restrictive</i> ] default values for security attributes that are used to enforce the SFP.
<b>10. FMT_MSA.3.2</b>	The TSF shall allow the [administrator] <b><u>which is user definable</u></b> to specify alternative initial values to override the default values when an object or information is created.
<b>FMT_SMR.1 Security Roles</b>	
<b>11. FMT_SMR.1.1</b>	The TSF shall maintain the roles [the authorized identified roles] <b><u>which is user definable and referred as a security group id</u></b> .
<b>12. FMT_SMR.1.2</b>	The TSF shall be able to associate users with roles.
<b>FMT_SMF.1 Specification of management Functions</b>	
<b>13. FMT_SMF.1.1</b>	<p>The TSF shall be capable of performing the following management functions: [User Account Profile Maintenance, User Password Management, User Group Management].</p> <p>*Application Note:User Account Profile provides the User Profile maintenance and user password management. Security Group screen provide User Group Management functionality.</p>
<b>FMT_MTD.1 Management of TSF Data</b>	
<b>14. FMT_MTD.1.1</b>	The TSF shall restrict the ability to [ <i>query, modify, delete, add</i> ] the [Security Group ID, Module ID Accessible by a security group, and user ID that belongs to the security group] to [administrator] <b><u>which is user definable</u></b>
<b>FMT_REV.1 Revocation</b>	
<b>15. FMT_REV.1.1</b>	The TSF shall restrict the ability to revoke [ <i>user account, user password</i> ] associated with the [ <i>users</i> ] under the control of the TSF to [Administrator]
<b>16. FMT_REV.1.2</b>	The TSF shall enforce the rules [ <i>Expiry Date of User Account, Account Disabled</i> ].
<b>FMT_SAE.1 Time-limited authorization</b>	

<b>17. FMT_SAE.1.1</b>	The TSF shall restrict the capability to specify an expiration time <b>(default: 90 days)</b> for [User Password] to [administrator] <b>which is user definable</b>
<b>18. FMT_SAE.1.2</b>	For each of these security attributes, the TSF shall be able to [restrict user login] after the expiration time for the indicated security attribute has passed

Table 9: Security Management

#### 5.1.4 FDP User Data Protection

<b>FDP_ACC.1 SubSet Access Control</b>	
<b>19. FDP_ACC.1.1</b>	The TSF shall enforce the [access control SFP] on [security group, user, TOE modules].
<b>FDP_ACF.1 Security Attribute Based Access Control</b>	
<b>20. FDP_ACF.1.1</b>	The TSF shall enforce the [access control SFP] to objects based on the following: [user id, security groups ID, module ID of SFP-relevant security attributes] <b>which is user definable</b>
<b>21. FDP_ACF.1.2</b>	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [access control to modules will be determined by the security group that particular user belongs].
<b>22. FDP_ACF.1.3</b>	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [none].
<b>23. FDP_ACF.1.4</b>	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [none].

Table 10: User Data Protection

## 5.2 Target of Evaluation (TOE) Security Assurance Requirement

The TOE meets the assurance requirements for EAL1 (Evaluation Assurance Level 1). These requirements are summarized in the following table:

Assurance Class	Component ID	Component Title
ADV: Development	ADV_FSP.1	Basic functional specification
AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC: Life-cycle support	ALC_CMC.1	Labeling of the TOE
	ALC_CMS.1	TOE CM coverage
ASE: Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.1	Security objectives for the operational environment
	ASE_REQ.1	Stated security requirements
	ASE_TSS.1	TOE summary specification
ATE: Tests	ATE_IND.1	Independent testing - conformance
AVA: Vulnerability assessment	AVA_VAN.1	Vulnerability survey

**Table 11: EAL1 (Evaluation Assurance Level 1) Class, Component ID and Component Title**

## 5.3 Rationale for not addressing all dependencies

### **FPT\_STM.1:**

FPT\_STM.1 is a dependency of FAU\_GEN.1 and FMT\_SAE.1 that has not been included. Reliable time stamps are provided by the environment through an interface of the TOE. Time Stamps captured in TOE is derived from the operating system

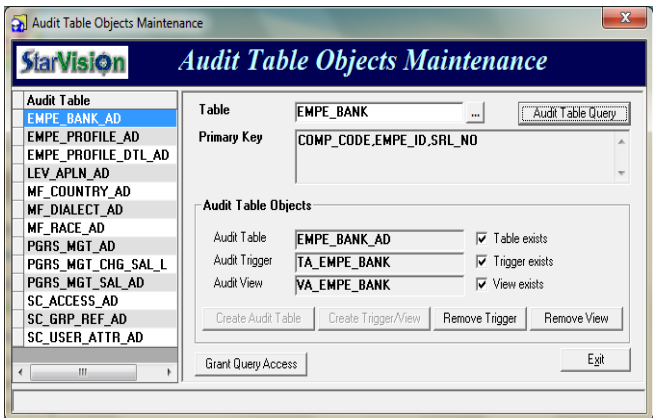
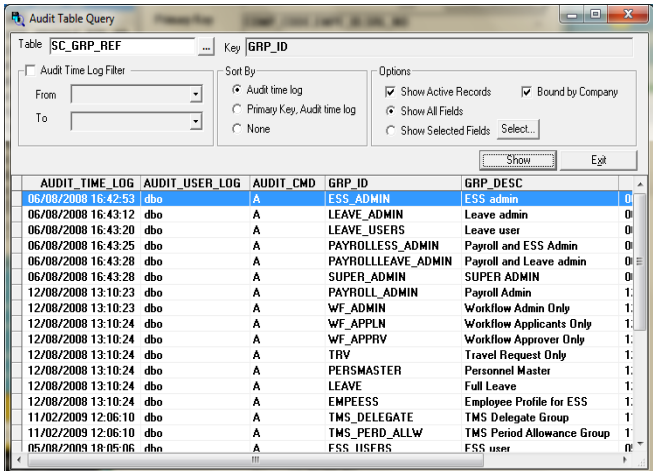
## 6 Target of Evaluation (TOE) Summary Specification

This section provides the TOE summary specification, a high-level definition of the security functions claimed to meet the functional and assurance requirements. It specifies the security functions defined earlier in section 5.1 (Security Functional Requirements) and also in Section 4 (Extended component Definition). It also specifies the mapping and relationship of the TSF logical scope with the Security Functional Requirements.

#	Security Functional Requirements	Audit Trail Utility	Session Log Viewer	Security Profile	Security Group	User Account Profile	Web Interface
1	FAU_GEN.1.1						Y
2	FAU_GEN.1.2						Y
3	FAU_SAR.1.1	Y	Y				
4	FAU_SAR.1.2	Y	Y				
5	FAU_SEL.1.1	Y		Y			
6	FIA_ATD.1.1					Y	
7	FMT_MOF.1.1				Y		
8	FMT_MSA.1.1				Y		
9	FMT_MSA.3.1				Y		
10	FMT_MSA.3.2				Y		
11	FMT_SMR.1.1				Y		
12	FMT_SMR.1.2				Y		
13	FMT_SMF.1.1				Y	Y	
14	FMT_MTD.1.1				Y		
15	FMT_REV.1.1					Y	
16	FMT_REV.1.2					Y	
17	FMT_SAE.1.1			Y			
18	FMT_SAE.1.2			Y			
19	FDP_ACC.1.1				Y		
20	FDP_ACF.1.1				Y		
21	FDP_ACF.1.2				Y		
22	FDP_ACF.1.3				Y		
23	FDP_ACF.1.4				Y		
24	FPT_STM_EXT.1.1	Y	Y	Y			
Sub Total		4	3	4	14	4	2

Table 12: Logical TSF and Security Functional Requirements Mapping

## Audit Trail Utility

No.	TSF Logical Scope: Audit Trail Utility	Security Functional Requirements	How it is Achieved
1	Audit Trail Utility	1. FAU_SAR.1.1	<p>Audit Review is achieved from the Audit Trail Utility. It provides the administrator or audit trail user to view and read specific event types and details.</p>  <p><b>Figure 2: Click on Audit Table Query table button to display Audit Trail data entries</b></p> <p>From Audit Trail Utility, click Audit Table Query button to display Audit Table Query screen that will display the audit trail data entries.</p>  <p><b>Figure 3: Audit Table Query screen showing audit trail data.</b></p>



No.	TSF Logical Scope: Audit Trail Utility	Security Functional Requirements	How it is Achieved
		2. FAU_SAR.1.2	The audit trail records are suitable to the user to interpret the information easily and can filter based accordingly.
		3. FAU_SEL.1.1	The Audit Table Query inside of Audit Trail Utility is allows the user to selectively filter the audit trail data based on user identity .
		4. FPT_STM_EXT.1.1	The time stamp captured in Audit Trail records are provided by the environment (Operating System).

Table 13: TSF Logical Scope - Audit Trail Utility and Security Functional Requirements Mapping

### Session Log Viewer

No	TSF Logical Scope: Session Log Viewer	Security Functional Requirements	How it is Achieved
2	Session Log Viewer	1. FAU_SAR.1.1	<p>User performed events related audit record can be reviewed from the Session Log Viewer. It provides the administrator or audit trail user to view and read specific event types and details.</p> <p>For example when a user login to the system, a line of record will be generated by the TOE and store in Session Log Table, which includes of the Time Log In, Event Type as Login, User that logged in. The content of this table can be viewed using Session Log Viewer by an administrator.</p>
		2. FAU_SAR.1.2	The event log displayed in the Session Log Viewer is suitable for the user to interpret the information easily and can be filtered accordingly, where user can use a query builder to filter the records. Sorting of the records can be done by clicking on the respective column name, by default clicking one will show the records sorted by that column in descending order, clicking on it again will sort the records in ascending order.
		3. FPT_STM_EXT.	Time stamp obtain from the environment (Operating

No	TSF Logical Scope: Session Log Viewer	Security Functional Requirements	How it is Achieved
		1 .1	System)



Table 14: TSF Logical Scope - Session Log Viewer and Security Functional Requirements Mapping

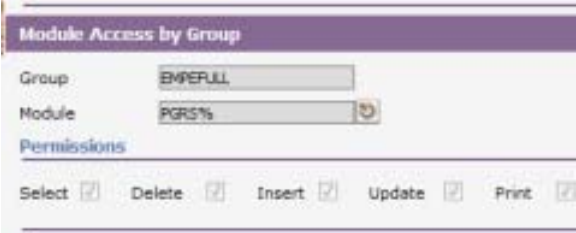
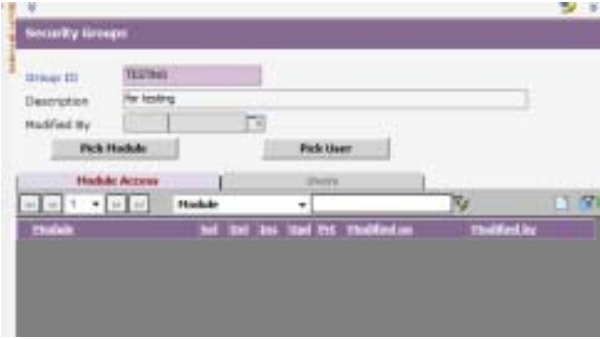
### Security Profile:

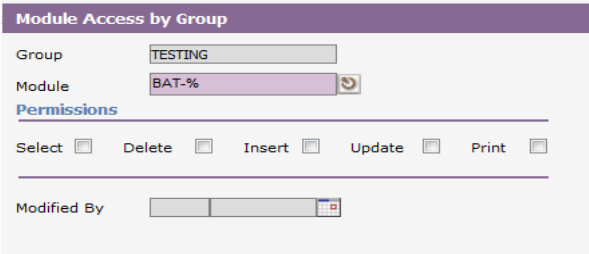

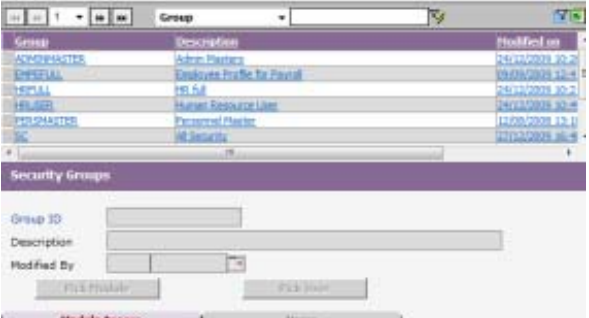
No	TSF Logical Scope: Security Profile	Security Functional Requirements	How it is Achieved
3	Security Profile	1. FMT_SAE.1.1	The expiration time is achieved via the User Account Profile. Expiration Date and Password Grace Logins After Expiry can be set.
		2. FMT_SAE.1.2	TOE restrict the user from login after the expiration time
		3. FPT_STM_EX T.1 .1	Time stamp obtain from the environment (Operating System).
		4. FAU_SEL.1.1	The Session Log viewer will allow the user to sort the audit trail records based on event type and session identity.

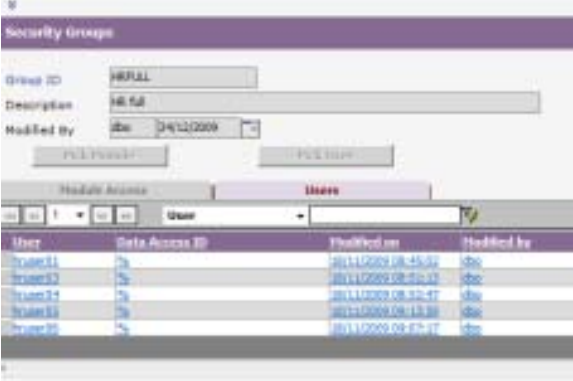
Table 15: TSF Logical Scope - Security Profile and Security Functional Requirements Mapping

**Security Group:**

<b>No</b>	<b>TSF Logical Scope: Security Group</b>	<b>Security Functional Requirements</b>	<b>How it is Achieved</b>
4	Security Group	1. FMT_MOF.1.1	<p>The restrictions functionality of the TOE is achieved via the Security Group screen. The Security Group screen allows a particular group (already defined) to enable or disable Select, Insert, Update, Delete and Print functions to a particular TOE module. The granted of access and privileges to module is assigned with two types of integer (“0” and “1”). On security group screen 1 is represented with a tick sign and 0 is empty.</p>  <p><b>Figure 4: Module Access by Group Screen in Security Group</b></p> <p>The user which was defined in the User Account Profile is then assigned to a particular group which was previously defined in the Security Group.</p>  <p><b>Figure 5: Screen of Security Group to list user that belongs to a group.</b></p>
		2. FMT_MSA.1.1	The access control is maintained in Security

No	TSF Logical Scope: Security Group	Security Functional Requirements	How it is Achieved
			<p>Group screen of the TOE. The access control can be applied to a group of user to perform add, query modify, delete and print on other Human Resource modules such as Promotion and Progress.</p>  <p>Figure 6: Module Access screen showing Permission for EMPEFULL group on Pgrs% module.</p>
		<p>3. FMT_MSA.3.1</p>	<p>By default when creating a new Security Group, no module is being allowed to be accessed. The administrator will need to add in respective module under that particular group to allow access rule to be set on those modules.</p>  <p>Figure 7: Create new Security Group, with no Module Access by Default</p> <p>All actions (select, update delete insert) are disabled by default when choosing a certain module, will require the administrator to check on the respective checkbox to allow the users under that security group to be able to perform that action upon that module.</p>

No	TSF Logical Scope: Security Group	Security Functional Requirements	How it is Achieved
			 <p data-bbox="800 640 1406 695"><b>Figure 8: Security Access, Module Access by Group Screen with no permission selected by default.</b></p>
		<p data-bbox="505 800 753 831">4. FMT_MSA.3.2</p>	<p data-bbox="800 800 1446 905">In Security group, administrator can check on the respective checkbox to overwrite the default value of disable all actions.</p>  <p data-bbox="800 1228 1446 1283"><b>Figure 9: Select and Delete permission were given to this group to act upon the selected module.</b></p>
		<p data-bbox="505 1314 753 1346">5. FMT_SMR.1.1</p>	<p data-bbox="800 1314 1435 1493">The security role is maintained in the Security Group Screen. The roles are defined based on the job function specified by the depending on job function (scope) defined by the customer (user definable).</p>  <p data-bbox="800 1816 1373 1871"><b>Figure 10: List of Groups (roles) maintained in Security Group module.</b></p>

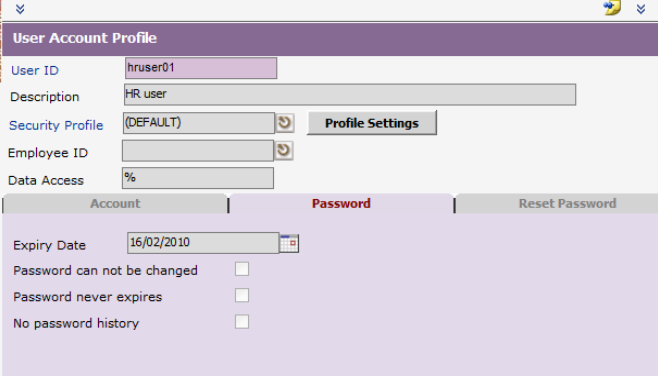
No	TSF Logical Scope: Security Group	Security Functional Requirements	How it is Achieved
		6. FMT_SMR.1.2	<p>The users are associated to the roles from the Security Group screen. It enables a particular user to be assigned to a particular type group (with roles assigned)</p>  <p>The screenshot shows a web application interface for 'Security Groups'. It includes fields for Group ID (HRFULL), Description (HR SA), and Modified By (HR/12/2009). Below these are buttons for 'FULL VIEW' and 'FULL VIEW'. A 'Module Access' section is visible, and a 'Users' tab is selected. A table lists users with columns for User, Data Access ID, Modification, and Modified by. The table contains several rows of data.</p> <p><b>Figure 11: User tie to roles in Security Group module.</b></p>
		7. FMT_SMF.1.1	<p>The TOE is able to allow or restrict access rights to certain user through the security group screen. Security group screen will allow administrator to perform user group management, by setting which user should belong in which group, and which group should have insert, delete, update, and select access to the tables.</p> <p>The functionality of User Profile and User Password management is provided by User Account Profile screen.</p>
		8. FMT_MTD.1.1	<p>The TOE is able to restrict the ability to query, modify, delete, add the Security Group ID, Module ID, User ID certain administrator through the security group screen.</p>
		9. FDP_ACC.1.1	<p>The enforcement of Security Group access control is applicable to TOE Security Group, User and modules.</p>
		10. FDP_ACF.1.1	<p>The enforcement of a user's access control to named groups of SFP objects (Security Groups</p>

No	TSF Logical Scope: Security Group	Security Functional Requirements	How it is Achieved
			ID, Users ID, Modules ID) which is user definable
		11. FDP_ACF.1.2	<p>The rules that control the Security Group access is a user's access in a TOE is depends on the security group he belongs to, and the access right to the TOE modules that is listed under that security group.</p> <p>Changes of the security group a user belongs to, or changes to the module can be access by a security group, can be controlled and edited by the TOE administrator.</p>
		12. FDP_ACF.1.3	No additional rules for explicitly authorize access of object or subjects.
		13. FDP_ACF.1.4	No additional rules for explicitly deny access of object or subjects.

Table 16: TSF Logical Scope - Security Group and Security Functional Requirements Mapping

**User Account Profile:**

No	TSF Logical Scope: User Account Profile	Security Functional Requirements	How it is Achieved
5	User Account Profile	1. FIA_ATD.1.1	<p>The security attributes belonging to individual users is defined and maintained in the User Account Profile. The following type of attributes is defined.</p> <ul style="list-style-type: none"> <li>• User ID (login ID)</li> <li>• Employee ID</li> <li>• Description (usually use as full name)</li> <li>• Security Profile</li> <li>• Data Access</li> <li>• User Password</li> <li>• User Group</li> </ul>

No	TSF Logical Scope: User Account Profile	Security Functional Requirements	How it is Achieved
			<ul style="list-style-type: none"> <li>• Account Effective Date</li> <li>• Account Expiry Date</li> <li>• Password Expiry Date</li> <li>• Password History checking (enable/disable)</li> </ul>  <p><b>Figure 12: User account in displayed in User Account Profile.</b></p>
		<p>2. FMT_SMF.1.1</p>	<p>User Account Profile screen allows administrator to perform user profile maintenance and user password management, such as creation of new user, reset password for user, revoke of user account by disable their account.</p> <p>User Account Profile also provide those functionality for user group management such as adding, removing of the security group the user belongs to.</p>
		<p>3. FMT_REV.1.1</p>	<p>The termination the user account is achieved within the User Account Profile.</p> <p>It is assume roles without access to security module are the roles that is not able to modify any user account or security group settings.</p> <p>However the TOE will restrict a user from editing his/her own user account related settings, and</p>



No	TSF Logical Scope: User Account Profile	Security Functional Requirements	How it is Achieved
			<p>resetting of his own password from the user account profile module.</p> <p>If a user would need to change his/her own password, it must be done through the login screen.</p>
		4. FMT_REV.1.2	<p>The enforce rules of the Expiry Date of User Account and Account disabled is achieved via User Account Profile, where the TOE will follow the setting specified in user account profile screen.</p>

Table 17: TSF Logical Scope - User Account Profile and Security Functional Requirements Mapping

**Web Interface:**

No	TSF Logical Scope: Web Interface	Security Functional Requirements	How it is Achieved
6	Web Interface	1. FAU_GEN.1.1	<p>Generation of audit trail logs is being done by web screen load function, which is a common function, exist across all web interface and executed upon opening of webpage, which can be start-up and shut down through the configuration settings at the Security Profile screen.</p> <p>Generation of the session logs are based on the user's actions perform on the web interfaces such as login to the TOE, opening of a screen, screen fetching, adding of a new record on that screen, delete of record from that screen, update of existing record on that page, and logout from the TOE.</p> <p>Generation of Audit Trail record, which consist of exactly on that user event which data has been changed, is triggered by a database trigger set against the screen's main table, upon a user action</p>

No	TSF Logical Scope: Web Interface	Security Functional Requirements	How it is Achieved
			<p>on that screen is perform, a similar copy of record will be recorded into the specific audit trail table of the related screen.</p>
		<p>2. FAU_GEN.1.2</p>	<p>Each generated session log consist of the date and time of the event, user identity, type of event, event action outcome and is viewable via the Session Log Viewer.</p> <p>For detailed audit trail records, which comes with detailed data changed, can be viewable from Audit Trail Utility – Audit Table Query screen. Each of this audit trail record includes the following fields: date and time action performed, user identity of the user that performed the event of updating the record, and the audit command that resembles the event type on which type of action he is performing onto that particular line record.</p>

**Table 18: TSF Logical Scope – Web Interface and Security Functional Requirements Mapping**