Oracle Corporation

Oracle Identity Governance 12c

Assurance Activity Report

Version 0.8

Oct, 2024

Document prepared by

www.lightshipsec.com

Table of Contents

1 Introduction

1 This Assurance Activity Report (AAR) documents the evaluation activities performed by Lightship Security for the evaluation identified in Table 1. The AAR is produced in accordance with National Information Assurance Program (NIAP) reporting guidelines.

1.1 Evaluation Identifiers

Table 1: Evaluation Identifiers

Scheme	Canadian Common Criteria Scheme
Evaluation Facility	Lightship Security
Developer/Sponsor	Oracle Corporation
TOE	Oracle Identity Governance 12c Build: 12.2.1.4.0
Security Target	Oracle Identity Governance 12c Security Target, v1.5
Protection Profile	Standard Protection Profile for Enterprise Security Management Identity and Credential Management (PP_ESM_ICM), v2.1

1.2 Evaluation Methods

2 The evaluation was performed using the methods, and standards identified in Table 2.

Table 2: Evaluation Methods

Evaluation Criteria	CC v3.1R5
Evaluation Methodology	CEM v3.1R5
Interpretations	**ESM ICM v2.1**

TD0844 - Addition of Assurance Package for Flaw Remediation V1.0 Conformance Claim	Not Applicable – No additional packages have been claimed.
TD0794 - Correction to FCS_SSH_EXT.1.7 Test 2	Not Applicable – SSH is not claimed.
TD0621: Corrections to FCS_TLS_EXT.1 in ESM PPs	Not Applicable – TLS is in the environment.
TD0576: FTP_ITC and FTP_TRP Updated	
TD0574: Update to FCS_SSH in ESM PPs	Not Applicable. The TOE does not implement SSH.

	TD0573: Update to FCS_COP and FCS_CKM in ESM PPs	Not Applicable. Cryptography is done in the environment.
	TD0079: RBG Cryptographic Transitions per NIST SP 800-131A Revision 1	Not Applicable. Cryptography is done in the environment.
	TD0066: Clarification of FAU_STG_EXT.1 Requirement in ESM PPs	
	TD0055: Move FTA_TAB.1 to Selection-Based Requirement	
	TD0042: Removal of Low-level Crypto Failure Audit from PPs	

1.3 Reference Documents

Table 3: List of Reference Documents

Ref	Document
[ST]	Oracle Identity Governance 12c Security Target, v1.5
[AGD]	Oracle Identity Governance 12c Common Criteria Guide, Version 1.4
[AGD-Self]	Oracle™ Fusion Middleware Performing Self Service Tasks with Oracle Identity Governance, 12c (12.2.1.4.0), E95920-08
[AGD-Admin]	Oracle™ Fusion Middleware Administering Oracle Identity Governance, 12c (12.2.1.4.0), E95926-14
[AGD-Help]	Oracle™ Fusion Middleware Help Topics for Oracle Identity Governance, 12c (12.2.1.4.0), E95917-05
[PP]	Standard Protection Profile for Enterprise Security Management Identity and Credential Management (PP_ESM_ICM), v2.1

2 Evaluation Activities for SFRs

2.1 Class ESM: Enterprise Security Management

2.1.1 ESM_EAU.2 Reliance on Enterprise Authentication

2.1.1.1 TSS

3 The evaluator shall check the TSS in order to determine that it describes the TSF as requiring authentication to use and that it describes, for each type of user or IT entity that authenticates to the TOE, the identification and authentication mechanism that is used. The evaluator shall also check to ensure that this information is appropriately represented by iterating the SFR for each authentication mechanism that is used by the TSF.

Findings:	[ST] Section 6.1.1 specifies “In order to manage the TOE, administrators must provide valid authentication credentials. The TOE uses the identity store in the Operational Environment to define its administrators, so they can authenticate to the TOE by using the same username/password that they use to access other organizational resources. Administrators provide a username and password to the TOE through an administrative interface. The TSF then initiates an authentication request to the environmental identity store (OID, or OUD) using LDAP.” This information describes the authentication to the TOE and the authentication mechanism used.

2.1.1.2 Guidance

4 The evaluator shall check the operational guidance in order to determine how the TOE determines whether an interactive user requesting access to it has been authenticated and how the TOE validates authentication credentials or identity assertions that it receives. If any IT entities authenticate to the TOE, the evaluator shall also check the operational guidance to verify that it identifies how these entities are authenticated and what configuration steps must be performed in order to set up the authentication.

Findings:	[AGD] Section 3.1.1 specifies that the TOE uses the Oracle Unified Directory (OUD) to authenticate administrative users. [AGD] Section 2.5.2 specifies the creation of an LDAP profile to interface with the OUD.

2.1.1.3 Tests

5 The evaluator shall test this capability by accessing the TOE without having provided valid identification and authentication information and observe that access to the TSF is subsequently denied. If any IT entities authenticate to the TOE, the evaluator shall instruct these IT entities to provide invalid identification and authentication information and observe that they are not able to access the TSF.

6 Note that positive testing of the identification and authentication is assumed to be tested by other requirements because successful authentication is a prerequisite to manage the TSF (and possibly for the TSF to interact with external IT entities).

High-Level Test Description
The evaluator attempted to access TOE services without providing valid combination of username and password. This was done by using a valid username and invalid password, and an invalid username and valid password. The evaluator then verified that access is permitted only by entering a valid username and valid password. The evaluator performed additional tests by navigating directly to protected URLs without authentication.
Findings: PASS

2.1.2 ESM_EID.2 Reliance on Enterprise Identification

7 Assurance Activity:

8 This functionality—for both interactive users and authorized IT entities—is verified concurrently with ESM_EAU.2.

2.1.3 ESM_ICD.1 Identity and Credential Definition

2.1.3.1 TSS

9 The evaluator shall review the TSS to verify that it identifies compatible ESM products and describes the identity and credential data that are used by those products. The evaluator shall review public documentation for compatible products and verify that they actually use the data in the compatible way asserted by the TSS.

Findings:	[ST] Section 6.1.2 specifies a list of ESM products which can use the identity and credential data. The evaluator reviewed public information for each of the products and verified that the product is able to communicate with the TOE over LDAP or another protocol, the evaluator additionally noted that the products listed each had an associated identity connector which enables the transfer of data. In the evaluated configuration the TOE will communicate with an instance of Oracle Unified Directory over LDAP.

2.1.3.2 Guidance

10 The evaluator shall review the operational guidance in order to verify that it indicates how identity and credential data are supplied to the TOE and this data is identified.

Findings:	[AGD] Section 2.5.2 specifies the creation of an LDAP profile to interface with the OUD which includes the specification of the LDAP server name.

2.1.3.3 Tests

11 The evaluator shall test this capability by using the TOE to create identity and credential data and sending this data to the compatible ESM product(s) for consumption. These tests shall exercise each capability described in the SFR,

including the ability to enforce credential complexity requirements. The evaluator will then perform basic identity and credential-related actions[1] on the compatible ESM products that use the identity and credential data in order to confirm that the data was applied appropriately.

High-Level Test Description
Create a user and associate credentials on the TOE. Assign the user privileges associated with a test VM which allows login via the Oracle OUD authentication. Log into the test VM as that user with the associated credentials. The TOE creates the user and associated credentials on the Oracle OUD LDAP server.
Findings: PASS

12 With respect to the requirements regarding credential complexity: the evaluator shall examine the TSS and operational guidance in order to identify the form of credentials collected:

13 a. For password-based credentials, the evaluator shall identify that all password composition, configuration, and aging requirements specified in the ST are discussed in the TSS and AGD and test these capabilities one at a time (for example: set minimum password length to 6, observe that a 7 character password and a 16 character password are both accepted, then change the minimum length to 8, observe that a 7 character password is rejected but that a 16 character password is accepted)

14 b. For non-password based credentials, the evaluator shall perform a basic strength of function analysis to determine the solution space of the authentication mechanism and the frequency with which password attempts can be made. For example, if the authentication is a 4-digit PIN that can be attempted once an hour, this requirement would not pass. If the strength of the authentication mechanism can't be determined by strength of function metrics at face value (for example, if a biometric authentication mechanism is being used), the vendor shall provide some evidence of the strength of function.

High-Level Test Description
Use the WebUI to configure the password policy. Note this can only be configured via the WebUI and cannot be configured via the REST API. Use each of the interfaces to change user passwords. Verify the ability of the TOE to set minimum password length and password composition rules and verify that the password reuse rules are settable by an administrator and enforced by the TOE. For non-password-based credentials the evaluator reviewed the TOE settings to require 3 questions be correctly answered. The evaluator reviewed the set of words and verified that the use of three words is stronger than a password. For example the set of the three words “Correct Horse Battery” has more entropy than an 8 character password.
Findings: PASS

[1] That is, exhaustive testing of edge conditions is not required.

2.1.4 ESM_ICT.1 Identity and Credential Transmission

2.1.4.1 TSS

15 The evaluator shall check the TSS in order to determine that the assignments were completed in a manner that is consistent with the guidance provided by the application note(s). The evaluator shall also check the TSS to see that it describes the ESM data that the TSF transmits to other ESM products and the circumstances that cause it to be transmitted.

Findings:	[ST] Section 6.1.3 specifies that the TOE provides identity data to the Operational Environment upon creation and by configurable periodic synchronization, with a 5 minute default. The section further specifies that identity and credential elements, as well as user attributes are transmitted.

2.1.4.2 Guidance

16 The evaluator shall review the operational guidance to determine how to create and update identity, credential (and potentially object attribute) data, and the circumstances under which new or updated data are transmitted to consuming ESM products (and how those circumstances are managed, if applicable).

Findings:	[AGD] Section 3.1.3 specifies that "The primary purpose of OIG is to provide a method to administer the identity and credential data of organizational users. In addition to allowing for direct configuration of this data, collections of privileges known as entitlements can be defined that are automatically granted based on combinations of relevant identity data", as well as "Administrators can also modify user identity data by approving or rejecting requests that are initiated by users themselves." [AGD] Section 3.1.4 specifies that "When a change is made to user identity and/or credential data using OIG, the change is immediately pushed to the Identity Store."

2.1.4.3 Tests

17 The evaluator shall test this capability by obtaining the compatible ESM products.

18 Following the procedures in the operational guidance for both the ICM and other ESM products, the evaluator shall create the indicated data (i.e., identity, credential, and potentially object attribute data) and ensure that the defined data is transmitted and installed successfully in compatible ESM products[2], in accordance with the circumstances defined in the SFR. In other words, (a) if the selection is completed to transmit after creation of new data, then the evaluator shall create the new data and ensure that, after a reasonable window for transmission, the new data is installed; (b) if the selection is completed to transmit periodically, the evaluator shall create the new data, wait until the periodic period has passed, and then confirm that the new data is present in the appropriate ESM components; or (c) if the section is completed to transmit upon the request of a compatible Secure Configuration Management component, the evaluator shall create the data, use the Secure Configuration Management component to request transmission, and the confirm that the appropriate ESM components have received and installed the data. If the ST author has specified "other circumstances", then a similar test shall be executed to confirm transmission under those circumstances.

[2] For testing purposes, it is acceptable to group compatible ESM products into equivalence groups and provide an argument as to why testing one member from a group is sufficient to cover all members of the group.

High-Level Test Description
Create a user and associate credentials on the TOE. Assign the user privileges associated with a test VM which allows login via the Oracle OUD authentication. Wait 5 minutes for the transmission of the user and credential date to the OUD. Log into the test VM as that user with the associated credentials.
Findings: PASS

19 The evaluator shall then make a change to the previously created data, and then repeat the previous procedure to ensure that the updated data is transmitted to the compatible ESM components in accordance with the SFR-specified circumstances. Lastly, as updating data encompasses deletion of data, the evaluator shall repeat the process a third time, this time deleting the data to ensure it is removed as active data from the compatible ESM components.

20 Note: This testing will likely be performed in conjunction with the testing of ESM_ICD.1.

High-Level Test Description
Continuing from the previous test case modify the password then wait for 5 minutes for the update to process. Verify the password update by logging into the test VM. Finally delete the user created in the previous test case, wait for 5 minutes for the update to process. Verify the update was processed by attempting to log into the test VM and the attempt failing.
Findings: PASS

2.2 Security Audit (FAU)

2.2.1 FAU_GEN.1 Audit Data Generation

2.2.1.1 TSS

21 The evaluator shall check the TSS and ensure that it summarizes the auditable events and describes the contents of the audit records.

Findings: [ST] Section 6.2.1 provides a summary of the auditable events and the contents of the records as follows:

The auditable event types can be summarized as follows:

- Administrator login/logout
- Product configuration changes
- Startup/shutdown of product
- Establishment/disestablishment of cryptographic channels
- Failure to perform cryptographic operations

For each auditable event, the date, time, type, subject identity, and outcome of the event is logged.

2.2.1.2 Guidance

22 The evaluator shall check the operational guidance and ensure that it lists all of the auditable events and provides description of the content of each type of audit

record. Each audit record format type shall be covered, and shall include a brief description of each field. The evaluator shall check to make sure that every audit event type mandated by the PP is described and that the description of the fields contains the information required in FAU_GEN 1.2, and the additional information specified in Table 3.

Findings:	[AGD-Admin] specifies in section 20.6 a definition of the audit logging configuration and audit data.

23 The evaluator shall review the operational guidance, and any available interface documentation, in order to determine the administrative interfaces (including subcommands, scripts, and configuration files) that permit configuration (including enabling or disabling) of the mechanisms implemented in the TOE that are necessary to enforce the requirements specified in the PP. The evaluator shall document the methodology or approach taken to do this. The evaluator may perform this activity as part of the activities associated with ensuring the AGD_OPE guidance satisfies the requirements. Using this list, the evaluation shall confirm that each security relevant administrative interface has a corresponding audit event that records the information appropriate for the event.

Findings:	[AGD-Admin] specifies in section 20.5 information of the configuration of the audit logging on the TOE.

2.2.1.3 Tests

24 The evaluator shall test the TOE's audit function by having the TOE generate audit records for all events that are defined in the ST and/or have been identified in the previous two activities. The evaluator shall then check the audit repository defined by the ST, operational guidance, or developmental evidence (if available) in order to determine that the audit records were written to the repository and contain the attributes as defined by the ST.

25 This testing may be done in conjunction with the exercise of other functionality. For example, if the ST specifies that an audit record will be generated when an incorrect authentication secret is entered, then audit records will be expected to be generated as a result of testing identification and authentication. The evaluator shall also check to ensure that the content of the logs are consistent with the activity performed on the TOE. For example, if a test is performed that revokes a credential from a user, the audit log for the event should correctly indicate a revocation operation.

High-Level Test Description
This testing is done in conjunction with the exercise of other functionality.
Findings: PASS

2.2.2 FAU_STG_EXT.1 External Audit Trail Storage

2.2.2.1 TSS

26 The evaluator shall check the TSS in order to determine that it describes the location where the TOE stores its audit data, and if this location is remote, the trusted channel that is used to protect the data in transit.

Findings:	[ST] Section 6.2.2 specifies that the TOE stores audit files on the local system as well as transmits audit data to the RDBMS via TLS.

2.2.2.2 Guidance

27 The evaluator shall check the operational guidance in order to determine that it lists any configuration steps required to set up audit storage. If audit data is stored in a remote repository, the evaluator shall also check the operational guidance in order to determine that a discussion on the interface to this repository is provided, including how the connection to it is established, how data is passed to it, and what happens when a connection to the repository is lost and subsequently re-established.

Findings:	[AGD] Section 3.2.2 specifies "By default, audit data produced by OIG is stored in the environmental Oracle database. This is not configurable." as well as "Note that since an active database connection is required for OIG to function, it is not possible for a situation to occur where audit server communications are disrupted while OIG continues to be operational." [AGD] Section 2.5.1 specifies the configuration steps required to configure the TOE to communicate with the Oracle database over TLS.

2.2.2.3 Tests

28 The evaluator shall test this function in conjunction with testing of FAU_GEN.1 by confirming that the same set of audit records are received by each of the configured audit destinations. The evaluator shall also make the connection to the external audit storage unavailable, perform audited events on the TOE, re-establish the connection, and observe that the external audit trail storage is synchronized with the local storage. Similar to the testing for FAU_GEN.1, this testing can be done in conjunction with the exercise of other functionality. Finally, since the requirement specifically calls for the audit records to be transmitted over the trusted channel established by FTP_ITC.1, verification of that requirement is sufficient to demonstrate this part of this one.

High-Level Test Description
Verify the TOE communicates with the database server which acts as a remote audit log server. Then disable the database server interface. The TOE will become unresponsive as the TOE requires the database server to perform auditable actions.
Findings: PASS

2.3 Identification and Authentication (FIA)

2.3.1 FIA_USB.1 User-Subject Binding

2.3.1.1 TSS

29 The evaluator shall check the TSS in order to determine that it describes the security attributes that are assigned to administrators and the means by which the administrator is associated with these attributes, both during initial assignment and when any changes are made to them.

Findings:	[ST] Section 6.4.1 specifies that "The administrator's role is defined in the RDBMS and associated with the other identity information for that administrator by the TSF. Every time an administrator submits a request to the server via the web GUI, that request is checked on the back end by the server."

	This information clarifies that the role attribute is assigned to administrators and the administrator is associated with the role by elements within the RDBMS.

2.3.1.2 Guidance

30 The evaluator shall check the operational guidance in order to verify that it describes the mechanism by which external data sources are invoked and mapped to user data that is controlled by the TSF.

Findings:	The [AGD] Section 3.3.1 specifies "the Identity Store where administrator accounts are defined is configured during the association of OIG to the OUD authentication mechanism. The Oracle database used by OIG stores a replicated copy of the administrator identity data for the purpose of mapping the authenticated administrator to their assigned privileges. OIG's administrative authority is role-based. Each role has the ability to perform certain tasks and an administrator account can be assigned to more than one role."

2.3.1.3 Tests

31 The evaluator shall test this capability by configuring the TSF to accept user information from external sources as defined by the ST. The evaluator shall then perform authentication activities using these methods and validate that authentication is successful in each instance. Based on the defined privileges assigned to each of the subjects, the evaluator shall then perform various management tests in order to determine that the user authorizations are consistent with their externally-defined attributes and the configuration of the TSF's access control policy. For example, if a user who is defined in an LDAP repository belongs to a certain group and the TSF is configured such that members of that group only have read-only access to a certain set of data, the evaluator shall authenticate to the TSF as that user and verify that as a subject under the control of the TSF, they do not have write access to that data. This verifies that the aspects of the user's identity data that are pertinent to how the TSF treats the user are appropriately taken from external sources and used in order to determine what the user is able to do.

High-Level Test Description
Configure the TOE to associate a role with a LDAP group ID. Login to the TOE as a member of the group and verify that the user is able to access the TOE as a member of the associated role.
Findings: PASS

2.4 Security Management (FMT)

2.4.1 FMT_MOF.1 Management of Functions Behavior

2.4.1.1 TSS

32 The evaluator shall check the TSS in order to determine that the assignments were completed in a manner that is consistent with the guidance provided by the application note(s). The evaluator shall also check the TSS to see that it describes the ability of the TSF to perform the required management functions and the authorizations that are required to do this.

Findings:	[ST] Section 5.3.5 clearly relates the assignments made in FMT_MOF.1 with the management functions and management roles in FMT_SMF.1 and FMT_SMR.1. respectively.

	[ST] Section 6.5.1 specifies “The management functions that are defined for the TSF are mapped to the corresponding authorizations that are defined within OIG itself as well as the roles that are given those authorizations. Note that if a role has the permission to interact with a function or object as described by Table 14, the role also has the permission to “determine the behavior of” (i.e. view) that function or object. Also note that the Application Instance Viewer, Entitlement Viewer, Help Desk, Role Viewer, and User Viewer roles can only perform these management functions by approving the corresponding user self-service requests; they cannot actually initiate the functions directly.” This information links the ability to perform the functions to the authorization required to perform the function.

2.4.1.2 Guidance

33 The evaluator shall review the operational guidance in order to determine what restrictions are in place on management of these attributes and how the TSF enforces them. For example, if management authority is role-based, then the operational guidance shall indicate this.

Findings:	[AGD] Section 3.4.1 specifies “OIG relies on the environmental Identity Store as its external data source for administrative identity data. However, it also maintains a local copy of these records in the Oracle database for synchronization purposes. The database also stores the assigned administrative roles for each account. By default, these are mapped 1:1 to the administrator accounts. The default mapping can be overridden so that an administrator’s privileges are mapped to a different account defined within OIG. This is known as “ad hoc” linking.”

2.4.1.3 Tests

34 The evaluator shall test this function by accessing the TSF using one or more appropriately privileged administrative accounts and determining that the management functions as described in the ST and operational guidance can be managed in a manner that is consistent with any instructions provided in the operational guidance. If the TSF can be configured by an authorized and compatible Secure Configuration Management product, the evaluator shall also configure such a product to manage the TSF and use this product to perform the defined management activities. In addition, any access restrictions to this behavior should be enforced in a manner that is consistent with the relevant documentation. The evaluator shall test this by attempting to perform a sampling of the available management functions using one or more unprivileged accounts to observe that the activities are rejected or unavailable.

High-Level Test Description
Login to the TOE for each identified role and confirm that the TOE allows access to the management function. Additionally ensure that the user in that role is denied access to functions outside the role. A sampling approach was taken given the number of roles and functions defined in the ST. The sample included all management functions to ensure coverage for FMT_SMF.1. The sample also included positive and negative test cases for each management role to ensure coverage for FMT_SMR.1. The evaluator did not test every function for every role. The evaluator also tested the REST API in the same manner. Each function and each role were tested with positive and negative test cases.
Findings: PASS

2.4.2 FMT_SMF.1 Specification of Management Functions

2.4.2.1 TSS

35 The evaluator shall check the TSS in order to determine that it summarizes the management functions that are available.

Findings: [ST] Section 6.5.3 specifies that table 15 defines the set of management activities. Table 15 in [ST] Section 5.3.5 provides a list of the following management functions:

Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)
Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)
Definition of identity and credential data that can be associated with users (activate, suspend, revoke credential, etc.)
Management of credential status
Enrolment of users into repository
Configuration of circumstances in which transmission of identity and credential data (and object attributes, if applicable) is performed
Configuration of external audit storage location
Definition of default subject security attributes, modification of subject security attributes
Management of sets of users that can interact with security functions
Management of the users that belong to a particular role
Configuration of actions that require trusted channel (if applicable)
Configuration of actions that require trusted path (if applicable)

2.4.2.2 Guidance

36 The evaluator shall check the operational guidance in order to determine that it defines all of the management functions that can be performed against the TSF, how to perform them, and what they accomplish.

Findings: The [AGD] and [AGD-Self] specify the following management functions as claimed in the [ST]:

Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF) is specified in [AGD] Section 2.5 for IT entities, and specified in [AGD-Self] Section 15.2.

Definition of identity and credential data that can be associated with users (activate, suspend, revoke credential, etc.) specified in [AGD-Self] Section 15.

Management of credential status specified in [AGD-Self] Section 15.8.

Enrolment of users into repository status specified in [AGD-Self] Section 21.

Configuration of circumstances in which transmission of identity and credential data (and object attributes, if applicable) is performed is specified in [AGD] Section 2.5.

Configuration of external audit storage location is specified in [AGD] Section 2.5.

Definition of default subject security attributes, modification of subject security attributes specified in [AGD-Self] Section 15.

	Management of sets of users that can interact with security functions specified in [AGD-Self] Section 15. Management of the users that belong to a particular role specified in [AGD-Self] Section 16.5. Configuration of actions that require trusted channel (if applicable) specified in [AGD] Section 2.5. Configuration of actions that require trusted path (if applicable) specified in [AGD] Section 2.5.

2.4.2.3 Tests

37 The evaluator shall test this capability by accessing the TOE and verifying that all of the defined management functions exist, that they can be performed in the prescribed manner, and that they accomplish the documented capability.

High-Level Test Description
This testing was conducted as part of the testing for FMT_MOF.1 The testing in FMT_MOF.1 shows that all the defined management functions that all the defined management functions exist and that they can be performed in the prescribed manner.
Findings: PASS

2.4.3 FMT_SMR.1 Security Management Roles

2.4.3.1 TSS

38 The evaluator shall review the TSS to determine the roles that are defined for the TOE. The evaluator shall also review the TSS to verify that the roles defined by this SFR are consistently referenced when discussion how management authorizations are determined.

Findings:	[ST] Section 6.5.4 specifies the following roles defined for the TOE: “Application Instance Administrator, Application Instance Authorizer, Application Instance Viewer, Entitlement Administrator, Entitlement Authorizer, Entitlement Viewer, Help Desk, Organization Administrator, Role Administrator, Role Authorizer, Role Viewer, Self-Service (implicit), System Administrator, System Configurator, User Administrator, User Viewer”. This list is consistent with the assignment in section 5.3.5. [ST] Table 19 provides a description of each of the roles which is consistent throughout the [ST].

2.4.3.2 Guidance

39 The evaluator shall review the operational guidance in order to verify that it provides instructions on how to assign users to roles. If the TSF provides only a single role that is automatically assigned to all users, then the evaluator shall review the operational guidance to verify that this fact is asserted.

Findings:	[AGD-Self] Section 16 provides instructions on how to assign users to roles.

2.4.3.3 Tests

40 The evaluator shall test this capability by using the TOE in the manner prescribed by the operational guidance to associate different users with each of the available roles. If the TSF provides the capability to define additional roles, the evaluator shall create at least one new role and ensure that a user can be assigned to it. Since other assurance activities for management requirements involve the evaluator assuming different roles on the TOE, it is possible that these testing activities will be addressed in the course of performing these other assurance activities.

High-Level Test Description
This testing was conducted as part of the testing for FMT_MOF.1 The testing in FMT_MOF.1 shows that each available role can manage the TOE in the manner prescribed by the [AGD].
Findings: PASS

2.5 Protection of the TSF

2.5.1 FPT_APW_EXT.1 Protection of Stored Credentials

2.5.1.1 TSS

41 The evaluator shall examine the TSS to determine that it details all authentication data, other than private keys addressed by FPT_SKP_EXT.1, that is used or stored by the TSF, and the method used to obscure the plaintext credential data when stored. This includes credential data stored by the TOE if the TOE performs authentication of users, as well as any credential data used by the TOE to access services in the operational environment (such as might be found in stored scripts). The TSS shall also describe the mechanisms used to ensure credentials are stored in such a way that they are unable to be viewed through an interface designed specifically for that purpose, as outlined in the application note. Alternatively, if authentication data is not stored by the TOE because the authoritative repository for this data is in the Operational Environment, this shall be detailed in the TSS.

Findings:	[ST] Section 6.6.1 specifies that the TOE does not store any credential data. The section further specifies that the passwords used by the TOE are hashed and then encrypted. The security questions/answers data is also stored in the environment.

2.5.1.2 Guidance

42 There are no operational guidance activities for this SFR.

N/A	There are no assurance activities.

2.5.1.3 Tests

43 The evaluator shall test this SFR by reviewing all the identified credential repositories to ensure that credentials are stored obscured, and that the repositories are not accessible to non-administrative users. The evaluator shall similarly review all scripts and storage for mechanisms used to access systems in the operational environment to ensure that credentials are stored obscured and that the system is configured such that data is inaccessible to non-administrative users.

High-Level Test Description

High-Level Test Description
Login to the TOE's underlying operating system as a non-admin user and use grep to search for password data in the configuration files. Login to the OIG console and present queries to the credential repositories to attempt to cause passwords to be displayed. Login to the TOE's underlying operating system as a root user and output configuration showing the passwords are stored encrypted.
Findings: PASS

2.5.2 FPT_SKP_EXT.1 Protection of Secret Key Parameters

2.5.2.1 TSS

44 The evaluator shall examine the TSS to determine that it details how any pre-shared keys, symmetric keys, and private keys are stored and that they are unable to be viewed through an interface designed specifically for that purpose, as outlined in the application note. If these values are not stored in plaintext, the TSS shall describe how they are protected/obscured.

Findings:	[ST] Section 6.6.2 specifies "Keys and cryptographic parameter data used by the TSF at run-time is stored in plaintext in volatile memory only. The key data is stored in a keystore file within the environmental WebLogic server's domain configuration directory. The password for this keystore file is stored in the Credential Store within the RDBMS." [ST] Section 6.6.2 further specifies "There is no interface to the TOE that allows an administrator to access this data in the clear."

2.5.2.2 Guidance

45 There are no operational guidance or testing activities for this SFR.

N/A	There are no assurance activities.

2.6 Trusted Paths/Channels (FTP)

2.6.1 (TD0576) FTP_ITC.1 Inter-TSF Trusted Channel

2.6.1.1 TSS

46 The evaluator shall examine the TSS to determine that, for all communications with authorized IT entities identified in the requirement, each communications mechanism is identified in terms of the allowed protocols for that IT entity and the method of assured identification of the non-TSF endpoint. The evaluator shall also confirm that all protocols listed in the TSS are specified and included in the requirements in the ST.

Findings:	[ST] Section 6.3.2 specifies each of the IT entities that the TOE communicates with and specifies that TOE uses TLS to communicate. This section also specifies "Assured identification of each endpoint identified in Table 17 is through the use of X.509 certificates."

2.6.1.2 Guidance

47 The evaluator shall confirm that the guidance documentation contains instructions for establishing the allowed protocols with each authorized IT entity, and that it contains recovery instructions should a connection be unintentionally broken.

Findings:	[AGD] Section 2.5 specifies instructions for establishment of TLS connections with authorized IT entities.

2.6.1.3 Tests

48 The evaluator shall perform the following tests:

49 Test 1: The evaluators shall ensure that communications using each protocol with each authorized IT entity is tested during the course of the evaluation, setting up the connections as described in the guidance documentation and ensuring that communication is successful.

High-Level Test Description
The TOE maintains trusted channels to the Oracle Database server and OUD server, which are set up as per the evaluated configuration. They are constantly tested throughout the evaluation.
Findings: PASS

50 Test 2: For each protocol that the TOE can initiate as defined in the requirement, the evaluator shall follow the guidance documentation to ensure that in fact the communication channel can be initiated from the TOE or the authorized IT entities.

High-Level Test Description
Engage Wireshark over the appropriate interface. Log into the Oracle-DB machine and restart the service to clear out TLS session information (which will force a new handshake). Attempt to access a protected resource using a predefined LDAP user and a bad password. Examine Wireshark and verify that the TOE initiates TLS communications with the Oracle-DB and LDAP service. Examine Wireshark and verify that the traffic is encrypted.
Findings: PASS

51 Test 3: The evaluator shall ensure, for each communication channel with an authorized IT entity, the channel data is not sent in plaintext.

High-Level Test Description
The previous test case ensures the data is not sent in plaintext.
Findings: PASS

52 Test 4: The evaluators shall ensure that, for each protocol associated with each authorized IT entity tested during test 1, the connection is physically interrupted[HD1] [MS2] . The evaluator shall then ensure that when physical connectivity is restored, communications are appropriately protected.

High-Level Test Description
Physically disconnect the interface (disconnect from the remote end rather that from the TOE end to ensure that the TOE is unable to invoke any layer 2 carrier-sensing mechanism). Wait 5 seconds. Physically reconnect the remote logging server. Examine Wireshark and verify that the log interface continues to send encrypted Application Data packets.
Findings: PASS

53 Further assurance activities are associated with the specific protocols.

54 For distributed TOEs, the evaluator shall perform tests on all TOE components according to the mapping of external secure channels to TOE components in the Security Target.

High-Level Test Description
The TOE is not a distributed TOE.
Findings: N/A

2.6.2 (TD0576) FTP_TRP.1 Trusted Path

2.6.2.1 TSS

55 The evaluator shall check the TSS to ensure that it identifies the protocol(s) used to establish the trusted path and ensure they are consistent with those declared in the ST. In addition, the evaluator shall ensure that the TSS adequately describes the way the trusted communication path is protected.

Findings:	[ST] Section 6.7.2 specifies that TLS is used to secure communications for trusted paths. The evaluator verified that this is consistent with other SFRs in the [ST].

56 The evaluator shall also check the TSS to ensure that the ST author specifies whether remote administration is applicable to the TOE and if applicable, specifies all the methods of remote administration, along with how those communications are protected.

Findings:	[ST] Section 6.7.2 specifies that TOE implements a trusted path between the OIG web GUI and administrators (web browsers) using TLS.

2.6.2.2 Guidance

57 The evaluator shall confirm that the guidance documentation contains instructions for how users will interact with the TOE such as a web application via HTTPS. The evaluator shall also ensure that the guidance documentation discusses the mechanism by which a trusted path to the TOE is established and which environmental components (if any) the TSF relies on to assist in this establishment.

Findings:	[AGD] Section 2.5 specifies instructions for configuring the TOE to use TLS connections to secure trusted path connections.

58 If remote administration is applicable to the TOE per the TSS, the evaluator shall confirm that the guidance documentation contains instructions for establishing the remote administrative sessions for each supported method.

Findings:	[AGD-Self] Section 3.1 specifies the steps to access the TOE for remote administration.

2.6.2.3 Tests

59 The evaluator shall perform the following set of tests and where applicable, repeat for each remote administration method:

60 Test 1: The evaluator shall ensure that communications using each protocol with each authorized IT entity, including each remote administration method, is tested during the course of the evaluation, setting up the connections as described in the guidance documentation and ensuring that communication is successful.

High-Level Test Description
The TOE maintains a trusted path to the web interface which is set up as per the evaluated configuration. It is constantly tested throughout the evaluation.
Findings: PASS

61 Test 2: For communications using each protocol with each authorized IT entity and method of remote administration supported, the evaluator shall follow the guidance documentation to ensure that there is no available interface that can be used by a remote user to establish a remote administrative session without invoking the trusted path.

High-Level Test Description
Engage Wireshark over the appropriate interface. Log into the trusted path. Examine Wireshark and verify that the trusted path sends encrypted traffic after any initial plaintext protocol negotiation occurs.
Findings: PASS

62 Test 3: The evaluator shall ensure that for communications of each protocol with each authorized IT entity, and for each method of remote administration, the channel data is not sent in plaintext.

High-Level Test Description
The previous test case ensures the data is not sent in plaintext.
Findings: PASS

63 Test 4: The evaluators shall ensure that, for each protocol and remote administration method combination tested during Test 1, the connection is physically interrupted. The evaluator shall then ensure that when physical connectivity is restored, communications are appropriately protected.

High-Level Test Description

High-Level Test Description
Engage Wireshark over the interface being tested. Physically disconnect the interface (disconnect from the remote end rather that from the TOE end to ensure that the TOE is unable to invoke any layer 2 carrier-sensing mechanism). Wait 5 seconds. Physically reconnect the remote logging server. Examine Wireshark and verify that the web interface continues to send encrypted Application Data packets.
Findings: PASS

64 For distributed TOEs, regardless of the tests performed, the evaluator shall perform tests on all TOE components according to the mapping of trusted paths to TOE components in the Security Target.

High-Level Test Description
N/A The TOE is not a distributed TOE.
Findings: N/A

3 Appendix C - Architectural Variations and Additional Requirements

3.1 FMT_MTD.1 Management of TSF Data

3.1.1 TSS

65 The evaluator shall review the TSS in order to determine the repository in which the authentication data used by the TOE is stored. The evaluator shall also determine how communications with this repository is secured.

Findings:	[ST] Section 6.5.2 specifies that the TOE uses a single Identity Store for both user and administrators. The section also specifies that communications are secured with TLS.

3.1.2 Guidance

66 The evaluator shall review the operational guidance in order to determine that it includes the data that can be managed and who is able to manage this data. This can be separated over multiple roles to distinguish between user administration and self-service; for example, both a Security Administrator and a specific user may be able to modify that user's own password.

Findings:	[AGD] Section 3.4.2 specifies that "Non-administrative users can access OIG to perform modifications to their account information, which includes their identifying attributes and authentication data such as passwords and security questions/answers. A user can also initiate a change to their account, role, and/or entitlements data, which is then reviewed for approval by an administrator. The process by which a user performs these actions is described in detail in section 6.1 of [SELF]. Administrative approvals of user data change requests is described in section 8 of [SELF]. Additionally, administrators can manage the identity and credential data of other users directly, as described in section 3.1 of [HELP]." Note: The AGD refers to [AGD-Self] as [SELF] and [AGD-Help] as [HELP].

3.1.3 Tests

67 The evaluator shall test this capability by performing the identified management activities with authorized roles in order to determine that they are allowed. The evaluator shall also attempt to perform these activities with unauthorized roles in order to determine that they are not allowed. Finally, the evaluator shall verify that communications between the TSF and the authentication data repository are secured by repeating the testing for FTP_ITC.1 over the interface between the two components.

High-Level Test Description
Using each of the defined roles perform each of the permitted functions and verify the role has access to the function. Using each of the defined roles, attempt to perform a non-permitted function and verify the role does not have access to the function. This testing was conducted as part of FMT_MOF.1. The testing of FTP_ITC.1 included testing of the interface between the TOE and the authentication data repository.
Findings: PASS

4 Security Assurance Requirements

4.1 Class ADV: Development

4.1.1 Basic Functional Specification (ADV_FSP.1)

4.1.1.1 Assurance Activity:

68 There are no specific assurance activities associated with these SARs. The functional specification documentation is provided to support the evaluation activities described for each SFR, and for other activities described for AGD, ATE, and AVA SARs. The requirements on the content of the functional specification information is implicitly assessed by virtue of the other assurance activities being performed; if the evaluator is unable to perform an activity because the there is insufficient interface information, then an adequate functional specification has not been provided. For example, if the TOE provides the capability to configure the key length for the encryption algorithm but fails to specify an interface to perform this function, then the assurance activity associated with FMT_SMF would fail.

Findings:	The requirements on the content of the functional specification information are implicitly assessed by virtue of the other assurance activities being performed.

69 The evaluator shall verify that the TOE functional specification describes the set of interfaces the TOE intercepts or works with. The evaluator shall examine the description of these interfaces and verify that they include a satisfactory description of their invocation.

Findings:	The [AGD] Section 2.5 describes the interfaces to the TOE, including how to configure them for secure operation.

4.2 Class AGD: Guidance Documentation

4.2.1 Operational User Guidance (AGD_OPE.1)

4.2.1.1 Assurance Activity:

70 Some of the contents of the operational guidance will be verified by the assurance activities with each SFR. The following additional information is also required.

Findings:	The assurance activities for each SFR have been evaluated.

71 The operational guidance shall contain instructions for configuring the cryptographic engine associated with the evaluated configuration of the TOE. It shall provide a warning to the administrator that use of other cryptographic engines was not evaluated nor tested during the CC evaluation of the TOE.

Findings:	[AGD] Section 2.5.1.3 specifies the configuration of the cryptographic engine.

4.2.2 Preparative Procedures (AGD_PRE.1)

4.2.2.1 Assurance Activity:

72 As indicated in the introduction above, there are significant expectations with respect to the documentation—especially when configuring the operational environment to support TOE functional requirements. The evaluator shall check to ensure that the guidance provided for the TOE adequately addresses all platforms (that is, combination of hardware and operating system) claimed for the TOE in the ST.

Findings:	[ST] specifies a single platform and all documentation requirements have been met. Therefore, this requirement has been met.

4.3 Class ALC: Life Cycle Support

4.3.1 Labeling of the TOE (ALC_CMC.1)

4.3.1.1 Assurance Activity:

73 The evaluator shall check the ST to ensure that it contains an identifier (such as a product name/version number) that specifically identifies the version that meets the requirements of the ST. Further, the evaluator shall check the AGD guidance and TOE samples received for testing to ensure that the version number is consistent with that in the ST. If the vendor maintains a web site advertising the TOE, the evaluator shall examine the information on the web site to ensure that the information in the ST is sufficient to distinguish the product.

Findings:	The evaluator verified that the TOE is identified as the “Oracle Identity Self Service” in the graphical user interface. The ST, AGD and vendor website for distribution of the TOE are consistent in the naming of the TOE.

4.3.2 TOE CM Coverage (ALC_CMS.1)

4.3.2.1 Assurance Activity:

74 The “evaluation evidence required by the SARs” in this PP is limited to the information in the ST coupled with the guidance provided to administrators and users under the AGD requirements. By ensuring that the TOE is specifically identified and that this identification is consistent in the ST and in the AGD guidance (as done in the assurance activity for ALC_CMC.1), the evaluator implicitly confirms the information required by this component.

Findings:	The evaluator has reviewed the ST and guidance provided and verified that it meets the requirements laid out by the PP. This requirement has been implicitly met.

4.4 Class ATE: Tests

4.4.1 Independent Testing - Conformance (ATE_IND.1)

4.4.1.1 Assurance Activity:

75 The evaluator shall prepare a test plan and report documenting the testing aspects of the system. The test plan covers all of the testing actions contained in the body of this PP's Assurance Activities. While it is not necessary to have one test case per test listed in an Assurance Activity, the evaluators shall document in the test plan that each applicable testing requirement in the ST is covered.

Findings:	The evaluator has generated a test plan and test results documents with the required information.

76 The Test Plan identifies the platforms to be tested, and for those platforms not included in the test plan but included in the ST, the test plan provides a justification for not testing the platforms. This justification shall address the differences between the tested platform and the untested platforms, and make an argument that the differences do not affect the testing to be performed. It is not sufficient to merely assert that the differences have no affect; rationale shall be provided. If all platforms claimed in the ST are tested, then no rationale is necessary.

Findings:	The evaluator has generated a test plan and test results documents with the required information. The test platform used and that listed in the ST are identical.

77 The test plan describes the composition of each platform to be tested, and any setup that is necessary beyond what is contained in the AGD documentation. It should be noted that the evaluators are expected to follow the AGD documentation for installation and setup of each platform either as part of a test or as a standard pre-test condition. This may include special test drivers or tools. For each driver or tool, an argument (not just an assertion) is provided that the driver or tool will not adversely affect the performance of the functionality by the TOE and its platform. This also includes the configuration of the cryptographic engine to be used. The cryptographic algorithms implemented by this engine are those specified by this PP and used by the cryptographic protocols being evaluated (IPsec, TLS/HTTPS, SSH).

Findings:	The evaluator has generated a test plan and test results documents with the required information.

78 The test plan identifies high-level test objectives as well as the test procedures to be followed to achieve those objectives. These procedures include expected results. The test report (that could just be an annotated version of the test plan) details the activities that took place when the test procedures were executed, and includes the actual results of the tests. This shall be a cumulative account, so if there was a test run that resulted in a failure; a fix installed; and then a successful re-run of the test, the report would show a "fail" and "pass" result (and the supporting details), and not just the "pass" result.

Findings:	The evaluator has generated a test plan and test results documents with the required information.

4.5 Class AVA: Vulnerability Assessment

4.5.1 Vulnerability Survey (AVA_VAN.1)

4.5.1.1 Assurance Activity:

79 As with ATE_IND, the evaluator shall generate a report to document their findings with respect to this requirement. This report could physically be part of the overall test report mentioned in ATE_IND, or a separate document. The evaluator performs a search of public information to determine the vulnerabilities that have been found in this category of ESM application in general, as well as those that pertain to the particular TOE. The evaluator documents the sources consulted and the vulnerabilities found in the report. For each vulnerability found, the evaluator either provides a rationale with respect to its non-applicability, or the evaluator formulates a test (using the guidelines provided in ATE_IND) to confirm the vulnerability, if suitable. Suitability is determined by assessing the attack vector needed to take advantage of the vulnerability. For example, if the vulnerability can be detected by pressing a key combination on boot-up, for example, a test would be suitable at the assurance level of this PP. If exploiting the vulnerability requires an electron microscope and liquid nitrogen, for instance, then a test would not be suitable and an appropriate justification would be formulated.

Findings:	The evaluator has generated a vulnerability assessment document with the required information.