Oracle® Enterprise Governance, Risk and Compliance

Installation Guide

Release 8.6.5.4000

Part No. E55702-01

July 2014

ORACLE

Oracle Enterprise Governance, Risk and Compliance Installation Guide

Part No. E55702-01

Primary Author: David Christie

Contents

Preface

This Preface introduces the guides and other information sources available to help you more effectively use Oracle Fusion Applications.

Disclaimer

The information contained in this document is intended to outline our general product direction and is for informational sharing purposes only, and should be considered in your capacity as a customer advisory board member or pursuant to your beta trial agreement only. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle. This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle software license and service agreement, which has been executed and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

Other Information Sources

My Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/support/contact.html or visit http://www.oracle.com/accessibility/support.html if you are hearing impaired.

Use the My Oracle Support Knowledge Browser to find documents for a product area. You can search for release-specific information, such as patches, alerts, white papers, and troubleshooting tips. Other services include health checks, guided lifecycle advice, and direct contact with industry experts through the My Oracle Support Community.

Oracle Enterprise Repository

Oracle Enterprise Repository provides visibility into service-oriented architecture assets to help you manage the lifecycle of your software from planning through implementation, testing, production, and changes. In Oracle Fusion Applications, you can use the Oracle Enterprise Repository for:

- Technical information about integrating with other applications, including services, operations, composites, events, and integration tables. The classification scheme shows the scenarios in which you use the assets, and includes diagrams, schematics, and links to other technical documentation.
- Publishing other technical information such as reusable components, policies, architecture diagrams, and topology diagrams.

The Oracle Fusion Applications information is provided as a solution pack that you can upload to your own deployment of Oracle Enterprise Repository. You can document and govern integration interface assets provided by Oracle with other assets in your environment in a common repository.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/us/corporate/accessibility/index.html.

Comments and Suggestions

Your comments are important to us. We encourage you to send us feedback about Oracle Fusion Applications Help and guides. Please send your suggestions to oracle_fusion_applications_help_ww@oracle.com. You can use the Send Feedback to Oracle link in the footer of Oracle Fusion Applications Help.

1

Introduction

Oracle Enterprise Governance, Risk and Compliance (GRC) is a set of products that regulate activity in business-management applications. This document provides instructions for the installation (or upgrade) of the following GRC products:

- Oracle Enterprise Governance, Risk and Compliance Manager (EGRCM) forms a documentary record of a company's strategy for addressing risk and complying with regulatory requirements.
- Oracle Advanced Controls enables users to create "models" and "continuous controls." Two Advanced Controls applications run from within the GRC platform:
  - In Oracle Enterprise Transaction Controls Governor (ETCG), models and controls specify circumstances under which individual transactions display evidence of error, fraud, or other risk.
  - In Oracle Application Access Controls Governor (AACG), models and controls define conflicts among duties that can be assigned in a company's applications, and identify users who have access to those conflicting duties.

    AACG can also implement "preventive analysis" — it can evaluate controls as duties are assigned to users of the company's applications, preventing them from gaining risky access.
- Oracle Fusion Application Access Controls Governor (FAACG) is a specialized installation of AACG that applies access models and controls in Oracle Fusion Applications. If you intend to run FAACG, see the most recent edition of the *Oracle Governance, Risk and Compliance Certifications Document* to determine whether version 8.6.5.4000 is certified for use with Fusion. If not, revert to the most recently certified version until version 8.6.5.4000 is ready.
- Oracle Fusion GRC Intelligence (GRCI) extracts data from GRC for display in dashboards and reports.

You can install GRC on its own, or to be integrated with an OID LDAP server that manages GRC users. (OID stands for Oracle Internet Directory; LDAP for Lightweight Directory Access Protocol.)

You can embed a GRCI instance within GRC. To use GRCI, install GRC first (see chapter 2). Then integrate GRCI with GRC (see chapter 3).

Prerequisites

GRC 8.6.5.4000 is an upgrade in a series that begain with release 8.6.5.1000. You can install GRC 8.6.5.4000 only as an upgrade to GRC 8.6.5.3000 (specifically, build 3029).

Any GRC installation runs on a 64-bit Linux server and requires:

- An Oracle 11.2.0.3 database (in which, optionally, Real Application Clusters may be enabled). In it, a GRC schema must be created. If you implement GRCI, a Data Analytics (DA) schema must exist as well. The database that supports the GRC schema must use the AL32UTF8 character set.
- Java — Oracle JDK 1.7 or higher.
- Middleware — For GRC itself, WebLogic Server 12c (12.1.2) or Tomcat Application Server 7.0.47. If you use WebLogic Server (WLS), you also need Application Development Runtime (ADR) 12.1.2 and Repository Creation Utility (RCU) 12.1.2. In the 12c release, RCU is packaged with ADR.

  If you intend to run GRCI, you also need WLS 11g (10.3.6), installed with RCU 11.1.1.7 and ADR 11.1.1.7. This is true even if you use WLS 12c to support GRC itself.

  A special case: Only if you use Fusion Application Access Controls Governor, GRC runs with WebLogic 11g components — WLS 10.3.6, RCU 11.1.1.7, and Service Oriented Architecture (SOA) 11.1.1.7. (The use of SOA is not supported with any other implementation of GRC 8.6.5.4000.)

As an option, an OID LDAP server can manage GRC users.

It is assumed that you will reuse instances of these components installed and configured initially for GRC 8.6.5.1000 and reused for GRC 8.6.5.2000 and 8.6.5.3000.

If you implement AACG preventive analysis, a preventive enforcement agent (PEA) must be installed in each business application subject to AACG controls. However, you need not reinstall PEAs in application instances where they are already installed.

On the server or a client system, the following web browsers can display the GRC interface: Microsoft Internet Explorer 8.*x* or 9.*x* (with the Adobe SVG plugin available from http://www.adobe.com/svg/viewer/install/mainframed.html) or FireFox 24.

For details about supported components, see the *Oracle Enterprise Governance, Risk and Compliance Certifications Document*.

Recording Configuration Values

Make a note of certain configuration values for version 8.6.5.3000, as you will need to re-enter them for version 8.6.5.4000. All these values are displayed in the GRC Manage Application Configurations page. (Start GRC 8.6.5.3000, then select Navigator → Setup and Administration → Setup → Manage Application Configurations).

- In all cases, select a Properties tab and note values you will need to enter in a ConfigUI page during 8.6.5.4000 installation.
- Only if you use FAACG, and so run GRC with WebLogic and use SOA, select a Worklist tab and note values entered there.

- If you have set up GRC to work with an OID LDAP repository, select a User Integration tab and not values entered there.
- If you use GRCI, select an Analytics tab and note the values entered there.

Downloading Files

Create a staging directory on your GRC server. (Throughout this document, *<grc_stage>* represents the full path to this directory.)

To install or upgrade GRC, download a file called grc865_4045.zip to <grc_stage>, and extract its contents there. To validate your download, generate a checksum and compare it with a checksum value published in *Release Notes* for the instance you are installing. To generate a checksum, run the command *md5sum grc.ear*.

If you have not embedded GRCI in your GRC 8.6.5.3000 instance, but wish to do so for 8.6.5.4000, you may do so only if you created a Data Analytics (DA) schema for GRC8.6.5.1000 and upgraded it (reconneced it to GRC) for releases 8.6.5.2000 and 8.6.5.3000. If so, also download files called grc865_1616_OBIEE_ 1of3.tar.gz, grc865_1616_OBIEE_ 2of3.tar.gz, and grc865_1616_ OBIEE_3of3.tar.gz to <grc_stage>.

(To embed GRCI in GRC, your instance must run with WebLogic. If you use Tomcat, you can run GRCI only as a standalone application. You do not need the three grc865_1616_OBIEE files for standalone GRCI, or if you have already embedded GRCI in an earlier 8.6.5 instance.)

2

Installing GRC

In broad terms, installation of GRC 8.6.5.4000 involves these steps:

1. Ensure that two directories, for the storage of GRC report data and ETL data, are ready for use.
2. Remove some files installed for GRC 8.6.5.3000, and run a setup script.
3. Restart the WebLogic or Tomcat application server, then perform configuration steps in a GRC ConfigUI page.
4. Restart your application server to complete the installation.

No matter whether you use WebLogic or Tomcat, you will (as noted in chapter 1) reuse database, Java, and middleware components installed initially for GRC 8.6.5.1000.

Back up your database, schema, middleware components, and report and transaction ETL repositories.

GRC Repositories

For your earlier version of GRC, you should have created two "repositories" — directories that store data generated by GRC. A report repository stores copies of GRC reports that users schedule to be run. A second repository stores synchronization data used for transaction analysis.

Reuse these repositories for GRC 8.6.5.4000. Retain the contents of the transaction synchronization repository. Note the paths to the repositories, as you will need to supply them later as configuration values.

GRC with WebLogic

If you installed GRC to run with WebLogic Server, complete the following steps:

1. Stop the WebLogic Administration Server and (if any exist in your installation) managed servers.
2. During installation of earler GRC releases, a directory called grc865 was created, typically as a subdirectory of your middleware home directory (represented in this document as <MW_HOME>). Delete the contents of this directory.

3. Navigate to <grc_stage>/dist, and locate a grc.ear file.
4. Extract the contents of grc.ear into the grc865 directory.
5. Navigate to <grc_stage>/dist. From there, run the file grc_wls_setup.sh. Supply the path to the grc865 directory (into which you extracted the contents of the grc.ear file in step 4). For example:

   ```
   cmd> ./grc_wls_setup.sh <MW_HOME>/grc865
   ```

6. Remove content from the following directories. (In these paths, <grc_domain> represents the name of the WebLogic domain created for GRC during installation of version 8.6.5.1000, and <managed_server> is the name of a WebLogic managed server, if one was created during installation of version 8.6.5.1000.)

   <MW_HOME>/user_projects/domains/<grc_domain>/servers/AdminServer/logs
   <MW_HOME>/user_projects/domains/<grc_domain>/servers/AdminServer/cache
   <MW_HOME>/user_projects/domains/<grc_domain>/servers/AdminServer/tmp
   <MW_HOME>/user_projects/domains/<grc_domain>/servers/<managed_server>/logs
   <MW_HOME>/user_projects/domains/<grc_domain>/servers/<managed_server>/cache
   <MW_HOME>/user_projects/domains/<grc_domain>/servers/<managed_server>/tmp

7. Restart the WebLogic servers.

GRC with Tomcat

If you installed GRC to run with Tomcat Application Server, complete the following steps:

1. Shut down the Tomcat Application Server.
2. Remove the directory <TomcatHome>/webapps/grc and all its contents.
3. Remove the Catalina directory from the Tomcat work area (<TomcatHome>/work/Catalina). Delete the contents of <TomcatHome>/temp. Also delete Tomcat logs, located at <TomcatHome>/logs. (You may want to save them to another location.)
4. Navigate to <TomcatHome>/webapps and delete the grc.war file.
5. Navigate to <grc_stage>/dist. From there, run the file grc_tomcate_setup.sh. Supply the paths to the <grc_stage>/dist subdirectory, <TomcatHome>, and the full path to your Java home as parameters:

   ```
   cmd> ./grc_tomcat_setup.sh <grc_stage>/dist <TomcatHome>
   <JavaHomePath>
   ```

6. Start the Tomcat application server.

Installing a Driver for RAC

If Real Application Clusters (RAC) is enabled in your GRC database, you must set up a jdbc-oci driver. (If you do not use RAC, this section does not apply; skip ahead to the next section, "GRC Configuration.")

1. Shut down your web application server (WebLogic Administration Server and, if installed, managed server; or Tomcat application server).

2. In a web browser, go to http://www.oracle.com/technetwork/database/features/instant-client/index-097480.html. Select the Instant Client link for the platform on which you are installing, then find the Basic download for 11.2.0.3.0.
3. Download and unzip the package into a single directory, such as "instantclient."
4. Set the library loading path in your environment to this directory before starting the application. On many Linux platforms, LD_ LIBRARY_PATH is the appropriate environment variable.
5. Copy the file ojdbc6.jar from the instant client to <TomcatHome>/webapps/grc/WEB-INF/lib if you installed GRC to run with Tomcat, or to grc865/grc/WEB-INF/lib if you installed GRC to run with WebLogic. (In the latter case, grc865 is the home directory for your GRC installation See "GRC with WebLogic," page 2-1).
6. Restart your web application server.

GRC Configuration

Regardless of whether you use WebLogic or Tomcat, open a ConfigUI page to perform GRC-specific configuration:

1. Access GRC at

   `http://host:port/grc`

   In this URL, replace *host* with the fully qualified domain name (FQDN) of your GRC server. Select one of the following values for *port*:

   - If you use WebLogic 11g because you are installing GRC to run FAACG, enter the port number you chose for the GRC managed server as you created a WebLogic domain.
   - If you use WebLogic 12c, enter the port number you chose for the Administration Server as you created a WebLogic domain.
   - If you use Tomcat, replace *port* with 8080 (if you accepted the default value when you installed Tomcat) or your configured value (if you changed the default during Tomcat installation).
2. A ConfigUI page appears. In the Installation Configuration section, type or select appropriate property values:
   - User Name: Supply the user name for the GRC database.
   - Password: Supply the password for the GRC database.
   - Confirm Password: Re-enter the password for the GRC database.
   - Port Number: Supply the port number at which the GRC database server communicates with other applications.
   - Service Identifier: Supply the service identifier (SID) for the GRC database server, as configured in the tnsnames.ora file. Or, if your GRC database supports RAC, enter the RAC service name configured for your RAC database.
   - Server Name: Supply the FQDN of the database server. Or, if your GRC database supports RAC, enter RAC@<SCAN_NAME>, where <SCAN_NAME> is the IP address/host name of the SCAN address configured for your RAC database.
   - Maximum DB Connections: Default is 50. You can edit this value.

- Report Repository Path: Supply the full path to the Report Repository directory discussed in "GRC Repositories" on page 2-1.
- Log Threshold: Select a value that sets the level of detail in log-file entries. From least to greatest detail, valid entries are *error*, *warn*, *info*, *debug*, and *trace*. Select *trace* only if Oracle Support instructs you to do so.
- Transaction ETL Path: Enter the full path to the directory you created to hold ETL data used by Enterprise Transaction Controls Governor (see "GRC Repositories" on page 2-1).
- App Server Library Path: Enter the full path to the library subdirectory of your web application server. If you are installing GRC to run FAACG, set this value to <grc865>/grc/WEB-INF/lib. If you use Tomcat Application Server and intend to enable parallel processing (see step 4 below), set this field to the "lib/adf" subdirectory of the Tomcat home directory.

3. In the Language Preferences section of the ConfigUI page, select check boxes for up to twelve languages in which you want GRC to be able to display information to its users. "English (U.S.)" should be selected by default; do not deselect it.
4. In the Performance Configuration section of the ConfigUI page, select or clear check boxes:
   - Optimize Appliance-Based Operation: Select the check box to optimize performance if the GRC application and GRC schema reside on the same machine. Do not select this check box if the GRC application and schema do not reside on the same machine. When you select this check box, an ORACLE_HOME Path field appears. In it, enter the full, absolute path to your Oracle Home — the directory in which you have installed the Oracle database that houses the GRC schema.
   - Enable Graph Synchronization Date Limit: "Data synchronization" enables GRC to recognize data changes in each business application subject to models and controls. Although the process applies to AACG and ETCG, it works differently for the two applications.

     Either application recognizes "business objects," each of which is a set of related fields from a "datasource" (business application). ETCG distinguishes among three categories of business object — Transaction (in which records are created or updated frequently), and Operational and Configuration (consisting of master-data or setup records that change infrequently).

     For ETCG only, select the Enable Graph Synchronization Date Limit check box to cause the synchronization of Transaction business objects to operate only on records created or updated in datasources on or after a specified date.

     The setting of this check box has no effect on ETCG Operational or Configuration business objects, for which a synchronization run encompasses all records, no matter when they were created or updated. Moreover, AACG does not distinguish among business-object categories, and the setting of this check box has no effect on AACG synchronization runs.

     When you select the check box, a Transactions Created As Of field appears. In it, enter the cutoff date for the synchronization of ETCG Transaction business objects. When you click in the field, a pop-up calendar appears. Click

left- or right-pointing arrows to select earlier or later months (and years), and then click on a date in a selected month.

- Externalize Report Engine: Select the check box to enable the reporting engine to run in its own Java process, so that the generation of large reports does not affect the performance of other functionality. But select the check box only if you have installed GRC on hardware identified as "certified" in the *Oracle Enterprise Governance, Risk and Compliance Certifications Document*; clear the check box if you use hardware identified as "supported."
- Enable Parallel Processing: Select this check box to enable multiple jobs to run simultaneously. When you select the Enable Parallel Processing check box, two fields appear:

  In a Number of Cores Available for Processing field, enter the number of processor cores you wish to devote to parallel processing. GRC uses one core for each job, until as many cores as you specify here are in use.

  In a Maximum Megabytes of Physical RAM Available field, specify an amount of memory for use in parallel processing. Ensure that this value is at least 4,096 MB times the number of cores. GRC then divides the memory value by the core value to determine the actual amount of memory per core. As a rule of thumb, enter total RAM minus 8 GB; you may need to adjust this value if other processes run slowly.
- Enforce Allocated Analysis Time Per Filter: Select this check box, and enter a number in the Minutes field, to limit the time that transaction models and controls can run.

  A model or control consists of filters, each of which defines some aspect of a risk and selects transactions that meet its definition. When the Allocated Analysis Time feature is enabled, each filter runs no longer than the number of minutes you specify. If time expires, the filter passes records it has selected to the next filter for analysis, but ignores records it has not yet examined. So a filter may not capture every record that meets its definition, and the model or control results are labeled "partial" in GRC job-management pages.

  Once enabled here, this feature may be disabled for individual models (and for the controls developed from those models). This feature applies only to transaction models and controls, not to access models and controls, and not to EGRCM objects.

5. In the ConfigUI page, click on Actions → Save. GRC tests the values you've entered and, if they are valid, saves them. (If any are invalid, an error message instructs you to re-enter them.)
6. Exit the ConfigUI page.

Completing the Installation

With components in place and properly configured, complete the installation, in effect by running your web application server.

1. Shut down your server — the Administration Server if you're using WebLogic, or the Tomcat application server if you're using Tomcat. Then restart the server.

2. In a web browser, enter the GRC URL (see step 1 of "GRC Configuration" on page 2-3).
3. Wait for a pop-up message to report, "Database upgrade and initialization process complete." Click on its OK button.
4. You are redirected to a GRC logon page. Log on to the application. You can use the *admin* user ID, with a password established for that user ID during the installation of earlier GRC versions.

If you do not intend to run FAACG (you have installed GRC without SOA), and if you have not set up an external OID LDAP repository to manage users, basic GRC installation is complete. (You may, however, choose complete other procedures described later.)

If you do intend to run FAACG (and so you have installed GRC to run with SOA), or if you have set up an OID LDAP repository, complete these additional steps:

1. If you use SOA, ensure that the SOA Server is running.
2. In GRC, select Navigator → Setup and Administration → Setup → Manage Application Configurations.
3. If you need to configure SOA, select the Worklist tab and enter these values:
   - Worklist Server User Name: Keep the default value, *soaadmin*.
   - Worklist Server Password. Enter the password you created for the soaadmin user (during installation of GRC 8.6.5.1000).
   - Confirm Password: Re-enter the Worklist Server Password.
   - Worklist Server URL: http://*host*:*port*, in which *host* is the IP address of your SOA server, and *port* is its port number.
   - Worklist Server Protocol: Select the communications protocol —SOAP or RMI — used by the GRC application to send and receive SOA requests.
4. If you need to configure external OID LDAP, select the User Integration tab and enter the following values:
   - Enable Single Sign On: See "Integrating with Single Sign On Authentication" on page 2-7.
   - Enable Integration: Select the check box to permit integration with LDAP to occur.
   - User Name: Supply the user name (common name) to log in to the LDAP server. This user should have admin privileges.
   - Password: Enter the password for the user identified in the User Name field.
   - Confirm Password: Re-enter the password for the user identified in the User Name field.
   - Port: Enter the port number at which the LDAP server communicates with other applications.
   - Server Name: Enter the host name of the LDAP server.
   - Bind DN Suffix: Enter the "User Base DN."

- Enable SSL Authentication: Select the check box to allow GRC to access the LDAP server through SSL. The LDAP server must be configured to support SSL.
- Perform LDAP Recursive Search: Select the check box to search recursively for users in subfolders along with those in the base path specified in the Bind DN Suffix field.
- Unique User Identifier: uid

5. In the Manage Application Configurations page, click on Actions → Save. Then log off of GRC.
6. Stop the GRC Deployment in the WebLogic Console:
   a. Log in to the WebLogic Console at

      `http://host:port/console`

      Replace *host* with the FQDN of your GRC server, and *port* with the number you selected for the WebLogic Administration Server.
   b. From the Domain Structure menu, select Deployments.
   c. From the Deployment page, locate the GRC deployment and verify the state is Active.
   d. Click the checkbox next to the GRC deployment.
   e. From the toolbar, click Stop → Force Stop Now.
7. Start the GRC Deployment in the WebLogic Console:
   a. From the Domain Structure menu, select Deployments.
   b. From the Deployment page, locate the GRC deployment and verify the state is Prepared.
   c. Click the checkbox next to the GRC deployment.
   d. From the toolbar, click Start → Servicing All Requests.

Integrating with Single Sign On Authentication

Rather than use the GRC authentication system to authenticate GRC users, you can integrate GRC with Oracle Access Management (OAM) Single Sign On (SSO). To do so, you must have installed GRC to run with WebLogic; SSO is not supported in a GRC instance that runs with Tomcat. Moreover, you require not only OAM 11g, but also Oracle HTTP Server (OHS) 11g WebGate for OAM.

First, register OHS WebGate 11g Agent for OAM 11g:

1. Log on to the OAM console. Its URL is `http://<oam_host>:<oam_port>/oamconsole`, in which <*oam_host*> is the host name of the OAM server, and <*oam_port*> is its port number.
2. In the SSO Agent panel, click on New OAM 11g WebGate.
3. In the Create OAM 11g WebGate tab, enter the following values:
   - Name: Enter any value to create a name for the agent.

- Base URL: Enter `http://<host>:<port>`, in which <*host*> is the host name of the machine where Oracle HTTP Server 11g WebGate is installed, and <*port*> is its port number.
- Security: Select *Open*.
- Host Identifier: Enter either the Name or the Base URL value.
- Select the Auto Create Policies check box.
- In the Protected Resource List, add */grc*.

Leave the Access Client Password and User Defined Parameters fields blank, and leave the Virtual Host and IP Validation checkboxes unselected.

4. Click the Apply button.

Next, modify OHS to redirect to GRC.

1. On the server on which you've installed OHS, navigate to <MW_HOME>/Oracle_WT1/instances/instance1/config/OHS/ohs1.
2. Open the mod_wl_hos.conf file in a text editor and add the following information to it:

```
<IfModule weblogic_module>
  WebLogicHost <GRC_HOST_NAME>
  WebLogicPort <GRC_PORT_NUMBER>
  Debug ON
  WLLogFile /tmp/weblogic.log
</IfModule>

<Location /grc>
  SetHandler weblogic-handler
</Location>
```

   Replace <GRC_HOST_NAME> with the fully qualified domain name of your GRC server. Replace <GRC_PORT_NUMBER> with the port of your GRC managed server (if you created one to run FAACG) or your Administration Server (if you did not create a managed server).

3. Save and close the mod_wl_hos.conf file.
4. Restart the OAM server and WebGate.

Next, add the OAM Identity Asserter to the GRC domain:

1. Log in to the WebLogic Server Administration Console:

   `http://host:port/console`

   Replace *host* with the FQDN of your GRC server, and *port* with the number you selected for the WebLogic Administration Server.

2. Click Lock and Edit.
3. Click Security Realms (on the left under Domain Structure), then click myrealm.
4. In the Providers tab, click the New button, and enter *OAM Identity Asserter* for both Name and Type. Then click the OK button.
5. In the Providers tab, click the newly created OAM Identity Asserter.

6. In the Common tab, select:
   - ControlFlag: Required
   - Active Types — Choose: OAM_REMOTE_USER (deselect ObSSOCookie)

   Click the Save option.
7. Return to the Providers tab, click on DefaultAuthenticator, change the ControlFlag to SUFFICIENT, and click the Save option.
8. In the Providers tab, reorder the authentication providers so that OAM Identity Asserter is first, DefaultAuthenticator is second, and DefaultIdentityAsserter is third. Then click the OK button.
9. Click Activate Changes and restart the application server.

Finally, enable SSO in GRC:

1. Log on to GRC and select Navigator → Setup and Administration → Setup → Manage Application Configurations. Select the User Integration tab.
2. Select the Enable Single Sign On check box.

3

Integrating GRCI

Oracle Fusion GRC Intelligence (GRCI) makes use of Oracle Business Intelligence Enterprise Edition (OBIEE) and a Data Analytics (DA) schema. You can run GRCI only if the DA schema was created for a release of GRC that could be installed independently of earlier releases (in this case, 8.6.5.1000), then reconnected to GRC for each subsequent upgrade-only release of GRC (in this case, 8.6.5.2000 and 8.6.5.3000). Therefore, you are assumed (for the purposes of this chapter) to be upgrading an instance of GRCI already installed in GRC 8.6.5.3000.

You may install a "fresh" instance of GRCI only if a DA schema was created for release 8.6.5.1000 and reconnected for releases 8.6.5.2000 and 8.6.5.3000. If so, obtain version 8.6.5.1000 of the *GRC Installation Guide* and follow its instructions for installing OBIEE and supporting middleware components.

Preparing for the Upgrade

GRCI makes us of Oracle Business Intelligence Enterprise Edition (OBIEE), which in turn is supported by WebLogic middleware components.

- If your GRC instance runs with WebLogic, you completed an "embedded" GRCI installation. (You may also have installed a second, standalone OBIEE instance, for use in customizing GRCI.)
- If your GRC instance runs with Tomcat, you completed a standalone GRCI installation.

Regardless of whether you installed GRC to run with WebLogic 12c or Tomcat Application Server, you will have installed GRCI to run with WebLogic 11g components. As you upgrade to 8.6.5.4000, you will reuse the OBIEE and WebLogic 11g components. To complete the procedure, identify the following:

- <MW_HOME>: The complete path to the 11g middleware home that serves GRCI. (If you installed GRC to run with WebLogic, this is not the same as the 12c middleware home that serves GRC.)
- If you run GRC with WebLogic, the host name and port number of the GRC server for the instance from which you are upgrading. (This is typically the WebLogic Administration Server, although if you run FAACG it is a managed server.)

- If you run GRC with Tomcat, the Oracle Enterprise Manager URL and the Business Intelligence Enterprise Edition URL; the host name and port number for the WebLogic Administration Server that supports OBIEE and GRCI; the fully qualified domain name for the machine on which OBIEE is installed. (These values were set, and reported in an "Installation Completed" screen, during installation of middleware components that support standalone OBIEE and GRCI. Ideally, they were noted as your earlier GRCI version was installed.)
- The service identifier (SID) and schema name for the Data Analytics (DA) database schema that supports GRCI.

Connecting to the DA Schema

The GRC schema used by GRC supplies data to the DA schema used by GRCI. For this to happen, you need to enter connectivity information in GRC.

1. Log on to GRC (see step 1 of "GRC Configuration" on page 2-3). Select Navigator → Tools → Setup and Administration → Setup → Manage Application Configurations → Analytics.
2. In the Data Analytics Configuration section, enter values that identify the DA schema. (These are values that you noted earlier. See "Recording Configuration Values" on page 1-2.)
   - User Name: Supply the user name for the DA database.
   - Password: Supply the password for the DA database.
   - Confirm Password: Re-enter the password for the DA database.
   - Port Number: Supply the port number at which the database server communicates with other applications.
   - Service Identifier: Supply the service identifier (SID) for the database server.
   - Server Name: Supply the fully qualified domain name of the database server.
3. When you finish entering property values, click on Actions → Save. GRC tests the values you've entered and, if they are valid, saves them. (If any are invalid, an error message instructs you to re-enter them.)
4. Look for the prompt, "Successfully saved configuration values."

After that message appears, a one-time process runs in the background. It updates the DA schema tables and views. This process takes approximately fifteen minutes. Do not stop your WebLogic or Tomcat server during this period.

Once you have connected to the DA schema, set a schedule on which the schema is refreshed — on which the DA schema reads from the GRC schema. You can modify a schedule at any time. (A refresh can take up to 90 minutes to finish.) To create the schedule:

1. Select the Analytics tab of the Manage Applications Configurations page.
2. Click on the Schedule Data Analytics Update button.

3. A Schedule Parameter dialog opens. Enter values that set the name of the schedule, its start date and time, the regularity with which the DA schema should be refreshed, and an end date (if any). Then click on the Schedule button.
4. Click on Actions → Save.

To view the status of a scheduled refresh, go to Tools → Setup and Administration → Manage Jobs. To view the Data Analytics schedule, go to Tools → Setup and Administration → Manage Scheduling.

Configuring Intelligence in GRC

Within the GRC application, you need to enter values than enable GRC to connect to OBIEE, and you need to select "dashboards" in which GRC displays reports.

1. Log on to GRC (see step 1 of "GRC Configuration" on page 2-3). Select Navigator → Tools → Setup and Administration → Setup → Manage Application Configurations → Analytics.
2. In the GRC Intelligence Configuration section, supply the following values. (Again, these are values you noted earlier. See "Recording Configuration Values" on page 1-2.)
   - OBIEE Server Username: The user name configured for the WebLogic Administration Server.
   - OBIEE Server Password: The password for the OBIEE Server Username (the password configured for the WebLogic Administration Server).
   - OBIEE Server Port: If you use WebLogic, *9704*. If you use Tomcat, the port number used by the WebLogic Administration Server.
   - OBIEE Server Host: If you use WebLogic, the fully qualified domain name for the GRC host — the machine on which you installed GRC in Chapter 2. If you use Tomcat, the fully qualified domain name for the machine on which you installed OBIEE.
   - Root Context: *analytics*

   Leave the Enable SSL Authentication check box unchecked.
3. An Intelligence Page Configuration section displays a row for each dashboard you can display for GRC. (Each is identified as a "subtab" of an Intelligence tab that appears in, or in reference to, a major GRC page, such as the home page or an overview page for an object such as risk or continuous control.)
   - To enable a dashboard, click in its field in the Enable column so that a check mark appears. To disable it, double-click so that the check mark disappears.
   - To modify the display name of a dashboard, double-click in its field in the Display Label column. The field becomes write-enabled; enter the name you want to use.
   - The default display name for some dashboards is User Defined. Each of these dashboards is tied to a particular location in GRC. You may create

reports, add them to one of the User Defined dashboards, and then select the dashboard for use, in effect (if not in actuality) creating a new dashboard.

You may also edit existing reports or existing dashboards. To perform any of these customizations, you must use a standalone OBIEE instance, then transport customized reports or dashboards to your embedded GRCI instance. Creating or modifying reports, modifying dashboards, and moving dashboards and reports across OBIEE instances are standard OBIEE procedures. To complete them, follow instructions provided in OBIEE documentation.

4. A GRCI Intelligence Standard Mode Link Configuration section contains a single field, GRCI Intelligence Standard Mode URL. If you have installed a standalone instance of OBIEE, enter the URL for that instance.
5. When you finish entering values, click on Action → Save. If you've modified settings in the GRC Intelligence Configuration section, GRC tests the values you've entered and, if they are valid, saves them. (If any are invalid, an error message instructs you to re-enter them.)
6. Look for the prompt, "Successfully saved configuration values."

In addition, each GRC user who is to have access to GRCI must be granted one or more of three GRC job roles: GRC Intelligence Administrator Job Role, GRCM Embedded Intelligence Viewer Job Role, and CCM Embedded Intelligence Viewer Job Role. For information on adding job roles to GRC user accounts, see the *Enterprise Governance, Risk and Compliance User Guide*.

Testing the Installation

As a first test, ensure that you can open OBIEE:

- If your GRC instance runs with WebLogic, open a browser and go to http://*host*:9704/analytics (in which *host* is the FQDN of the machine on which you installed GRCI). Log in with your GRCI WebLogic Administration username and password.
- If your GRC instance runs with Tomcat, open a browser and go to your Business Intelligence Enterprise Edition URL. Log in with your WebLogic Administration username and password.

Second, ensure that the GRCI dashboard loads with no errors in your GRC application:

1. Ensure that the DA schema has been refreshed (see page 3-2).
2. Log on to GRC (see step 1 of "GRC Configuration" on page 2-3). Use the logon credentials of a user who has been assigned GRCI job roles.
3. Click on the Intelligence tab for each of the home and overview pages in which you've enabled a GRCI dashboard. (See step 3 of "Configuring Intelligence in GRC," page 3-3.)

If you see no errors, the integration has been successful.

4

Additional Advanced Controls Configuration

Once you've installed GRC 8.6.5.4000, complete additional configuration procedures as needed if you intend to use AACG or ETCG:

- Define information with which GRC creates "global users." Business applications subject to models and controls may have user-account information that varies from one application to the next. GRC maps each person's business-application IDs to a global-user ID. You can determine what information GRC uses to do so.

  However, version 8.6.5.4000 inherits the global-user definition from 8.6.5.3000. If you are satisfied with your configuration for the earlier version, you need not redefine it for version 8.6.5.4000.
- Decide whether to implement a Page Access Configurations business object, which enables AACG users to build models and controls that take PeopleSoft user preferences into account. This feature is enabled by default. If your access models and controls do not cite PeopleSoft user preferences, you can disable this feature to improve performance and reduce memory requirements.
- Set up datasources — connections to business applications in which GRC is to perform analysis. However, version 8.6.5.4000 inherits datasources configured for version 8.6.5.3000. For version 8.6.5.4000, you need to set up only new datasources.
- Complete the following procedures in the order indicated:

  1. Perform access synchronization on all datasources used for AACG analysis (see "How to Synchronize Data," page 4-6).
  2. Perform a graph rebuild on all datasources used for ETCG analysis (again, see "How to Synchronize Data" on page 4-6).
  3. Run all controls that compile data for user defined objects (controls for which the result type is "Dataset").
  4. Run all models and all controls that generate incidents (controls for which the result type is "Incidents").

  For information on running models and controls, and distinguishing between control types, see the user guides for AACG and ETCG.

Configuring Global Users

Implement one of the following options to determine the information GRC uses to create global users. Important: Select an option that identifies each person uniquely.

- EMAIL_ONLY: Match the global user to email addresses from distinct datasources (or within one datasource). This is the default.
- EMAIL_AND_USERNAME: Match the global user to email address plus username from distinct datasources (or within one datasource). This option is required for FAACG implementations. Because PeopleSoft implementations often do not use the email address for users, customers who implement PeopleSoft usually select this option as well.
- EMAIL_AND_ALL_NAMES: Match the global user to email address, username, given name, and surname from distinct datasources (or within one datasource).

GRC users regularly synchronize data and analyze controls to produce "incidents" (records of control violations). If no data has been synchronized and no controls have been analyzed on any of the 8.6.5.1000–8.6.5.4000 instances, complete the following three steps to change a global-user configuration.

1. Use SQL*Plus, or any other tool with the ability to execute SQL commands on a database, to connect to the GRC schema.
2. Run the following SQL statement:

```
DELETE FROM GRC_PROPERTIES
WHERE NAME like 'GLOBAL_USER_CONFIG';
COMMIT;
```

3. Run *one* of the following SQL statements, depending on the global-user format you want to implement:

   For email and username, run the following statement:

```
Insert into GRC_PROPERTIES (NAME, VALUE, DESCRIPTION, DEFAULT_VALUE,
VISIBLE, CONFIGURABLE, DATA_TYPE_ID)Values ('GLOBAL_USER_CONFIG',
'EMAIL_AND_USERNAME', 'Global User configuration. Possible values:
EMAIL_ONLY, EMAIL_AND_USERNAME, EMAIL_AND_ALL_NAMES', 'EMAIL_ONLY',
0, 0, 0);

COMMIT;
```

   For email, username, given name, and surname, run the following statement:

```
Insert into GRC_PROPERTIES (NAME, VALUE, DESCRIPTION, DEFAULT_VALUE,
VISIBLE, CONFIGURABLE, DATA_TYPE_ID) Values ('GLOBAL_USER_CONFIG',
'EMAIL_AND_ALL_NAMES', 'Global User configuration. Possible values:
EMAIL_ONLY, EMAIL_AND_USERNAME, EMAIL_AND_ALL_NAMES', 'EMAIL_ONLY',
0, 0, 0);

COMMIT;
```

   For email only, run the following statement. (As already noted, email-only is the default configuration. Run this statement only if you have changed your global-user configuration to one of the other formats, and want to change back.)

```
Insert into GRC_PROPERTIES (NAME, VALUE, DESCRIPTION, DEFAULT_VALUE,
VISIBLE, CONFIGURABLE, DATA_TYPE_ID) Values ('GLOBAL_USER_CONFIG',
'EMAIL_ONLY', 'Global User configuration. Possible values: EMAIL_ONLY,
EMAIL_AND_USERNAME, EMAIL_AND_ALL_NAMES', 'EMAIL_ONLY', 0, 0, 0);

COMMIT;
```

A second possibility is that data has been synchronized, but controls have not been analyzed on any of the 8.6.5.1000–8.6.5.4000 instances. If so, changing your global-user configuration wipes out all existing global-user data.

1. Complete the steps outlined above for the first global-user-configuration scenario (in which data synchronization and control analysis have not occurred).
2. Sill logged on to your SQL tool, also run the following SQL statement:

```
TRUNCATE TABLE GRC_SRC_USER_MAPPING;
TRUNCATE TABLE GRC_GLOBAL USER;
COMMIT;
```

A third possibility is that data has been synchronized, controls have been analyzed, and incidents have been generated on any of the 8.6.5.1000–8.6.5.4000 instances. In this case, when you change your global-user configuration, all existing incidents become invalid, and all existing global-user data is wiped out.

1. Log on to GRC (see page 2-3). Select Setup and Administration under Tools in the Navigator, then Manage Application Configurations under Setup. Select the Maintenance tab, and from the Maintenance page, purge *all* existing incidents. (For detailed instructions on purging incidents, see the *Governance, Risk and Compliance User Guide*.)
2. Still logged on to GRC, go to the Manage Results page. (Select Manage Incident Results from the Result Management tasks available under Continuous Control Management in the Navigator.) Select Incident Result in the View By list box, and confirm that no incidents exist.
3. Log off of GRC and shut down the application server.
4. Complete the steps outlined above for the first global-user-configuration scenario (in which data synchronization and control analysis have not occurred).
5. While logged on to your SQL tool, also run the following SQL statement:

```
TRUNCATE TABLE GRC_SUM_CTRL_INC;
TRUNCATE TABLE GRC_SRC_USER_MAPPING;
TRUNCATE TABLE GRC_GLOBAL USER;
COMMIT;
```

6. Clear the contents of your Transaction ETL Path folder. (This folder is specified as GRC properties are set. See page 2-3).

Enabling or Disabling Page Access Configurations

An access model or control may include filters that serve as conditions — they specify users or other objects that are exempt from analysis. Like any other access filter, a condition filter specifies a business object — a set of related fields from a datasource (business application). A business object called Page Access Configurations makes PeopleSoft user-preference values available for use in condition filters. By default, processing of data provided by this business object is enabled.

If your site does not use PeopleSoft user-preference values in access models and controls, you may choose to disable the processing of Page Access Configurations data. This improves performance and reduces memory requirements.

Important Note: If you disable Page Access Configurations data processing, the business object will nevertheless appear to be available for use in models. Users may create filters that cite this object, but GRC will ignore those filters. This may cause models (and controls developed from those models) to return results that differ from those that users expect. If you disable Page Access Configurations data processing, alert users not to use the Page Access Configurations business object as they create models.

To disable Page Access Configurations data processing:

1. Shut down the GRC application server.
2. Use SQL*Plus, or any other tool with the ability to execute SQL commands on a database, to connect to the GRC schema.
3. Run the following SQL statement

```
update GRC_PROPERTIES set VALUE = 'FALSE' where NAME =
'grc.access.user.preferences';
COMMIT;
```

4. Restart the GRC application server.

Configuring Datasources and Synchronizing Data

Connect GRC to datasources (instances of business-management applications that are to be subject to GRC models or controls). Also synchronize data for each data-source — collect information required for AACG or ETCG analysis.

Synchronization and Global Users

The order in which you synchronize access data from datasources determines how GRC creates global-user IDs: It adopts the ID configured for each user in the first datasource to be synchronized. When data from a second datasource is synchronized, GRC matches users who also exist in the first datasource to their already-existing global-user IDs. For each user who did not exist in the first datasource, GRC adopts the user ID from the second datasource as the user's global ID. And so on.

AACG pages display the global-user ID for each business-application user. You may prefer to set IDs from a particular datasource as the global-user IDs.

However, during an upgrade, GRC inherits the global-user IDs existing on the earlier version. For version 8.6.5.4000, global-user IDs are initially the same as they were for version 8.6.5.3000.

If you modify the global-user configuration (see page 4-2), existing global IDs are wiped out. In that case, or as you add new datasources, consider the following:

Configure all datasources in which you expect to apply AACG models and controls before you synchronize data for any of them. Next, choose a datasource from which you want GRC to adopt IDs as global-user IDs, and synchronize that datasource first. Establish an order for the remaining datasources, each of which sets global IDs for users who do not exist in the datasources for which synchronization has already been completed. Then synchronize the remaining datasources in that order.

To configure datasources or to synchronize their data, log on to GRC (see page 2-3). Select Setup and Administration under Tools in the Navigator, then Manage Application Datasources under Setup.

Special Cases Involving SQL Server

You must install the Microsoft JDBC Driver 4.0 for SQL Server if your GRC instance connects to a Microsoft SQL Server datasource and if either of the following is true:

- Your GRC instance runs with Tomcat Application Server.
- Your GRC instance runs with WebLogic and implements Secure Sockets Layer.

Install the driver before you synchronize data for the SQL Server datasource. However, if you are upgrading and have already competed this procedure for your earlier GRC version, you need not reinstall the driver.

On the GRC server:

1. Download the UNIX version of the JDBC driver — sqljdbc_*.tar.gz — from http://msdn.microsoft.com/en-us/data/aa937724.aspx.
2. Shut down your application server.
3. From the download file, extract the JDBC driver for SQL Server 2005 and newer — sqljdbc4.jar. (A SQL Server 2000 driver is also included in the download file, but is not supported by GRC.)
4. Copy the sqljdbc4.jar file to a directory appropriate for your application server:
   - If you use Tomcat, the directory is <TomcatHome>/webapps/grc/WEB-INF/lib.
   - If you use WebLogic, the directory is <MW_HOME>/user_projects/domains/<grc_domain>/lib
5. If you use WebLogic, edit the setDomainEnv.sh file, which is located in the <MW_HOME>/user_projects/domains/<grc_domain>/bin directory.

   Locate the following line:

   ```
   if [ "${PRE_CLASSPATH}" != "" ] ; then
   ```

   Immediately before that line, add the following line:

   ```
   PRE_CLASSPATH="<MW_HOME>/user_projects/domains/<grc_domain>
   /lib/sqljdbc4.jar"
   ```

   (Skip this step if you use Tomcat.)
6. Restart your application server.

How to Configure Datasources

To configure a datasource, complete these steps. However, remember that GRC version 8.6.5.4000 inherits datasources configured for version 8.6.5.3000, and you need not reconfigure them. (To set up a Fusion datasource, see page 5-2.)

1. In the GRC Manage Application Datasources page click on Actions → Create New. A Create Datasource window opens. Enter the following values:
   - Datasource Name: Create a name for the datasource.

- Description: Type a brief description of the datasource (optional).
- Application Type: Select the type of business application to which you are connecting, such as EBS or PeopleSoft.
- Application Type Version: Select the version number of the business-management application to which you are connecting.
- Default Datasource: Select the checkbox to make the datasource you are configuring the default for use in models. Only one datasource can have this value selected.
- Connector Type: For an Oracle EBS or PeopleSoft datasource, select Default. For any other application, you would need to have created and uploaded a custom connector; select it.
- Connector Properties: Enter values required for the connector you specified in Connector Type. Values vary by connector. They may include:
  - ERP Database Type: Select the type of database — Oracle, Oracle RAC, MS SQL Server, DB2, or MySQL — used by the business-management application being configured as a datasource.
  - Hostname: For Oracle EBS or PeopleSoft, supply the fully qualified domain name (FQDN) for the machine that hosts the database used by the business-management application. Or, if the database is RAC-enabled, enter RAC@<SCAN_NAME>, where <SCAN_NAME> is the IP address/host name configured for the RAC database.
  - Service Name: For Oracle EBS or PeopleSoft, supply the SID value configured for the business-application database in the tnsnames.ora file. Or, if the database is RAC-enabled, enter the RAC service name configured for the RAC database.
  - Port: For Oracle EBS or PeopleSoft, enter the port number that the business-application database uses to communicate with other applications.
  - Username: For Oracle EBS or PeopleSoft, supply the user name for the business-application database. (For an Oracle database, this is the same as Schema Name; for an Oracle EBS instance, this is typically APPS.)
  - Password: Supply the password that authenticates the user name for the business-application database.

2. After entering values, click on the Test Connection button.
3. When the test completes successfully, click the Save or Save and Close button. A row representing the datasource appears in the Manage Application Datasources grid.

How to Synchronize Data

You must synchronize data from every datasource used for access analysis, and "rebuild the graph" for every datasource used for transaction analysis — even datasources inherited from your earlier GRC version.

An ordinary synchronization run is incremental — it creates or updates only records that are new or have changed since the previous synchronization. A graph rebuild

deletes all data for a given datasource and replaces it with a complete set of current data. This typically takes longer than ordinary synchronization.

To synchronize access data, complete these steps:

1. In the Manage Application Datasources page, select the row for the access datasource with which you want to synchronize data.
2. Click on Actions → Synchronize Access.
3. A confirmation message appears; click its OK button.

To "rebuild the graph" for transaction data, complete these steps:

1. In the Manage Application Datasources page, select the row for a transaction datasource.
2. Select Actions → Rebuild Graph.
3. A confirmation message appears; click its OK button.

There is an option to synchronize transaction data; it's the preferred option for routine use of ETCG, but you would not use it in this instance because, during a GRC upgrade, you must perform a graph rebuild on transaction datasources. You can also select an option to schedule synchronization runs. For more on this, see the *Enterprise Governance, Risk and Compliance User Guide*.

Each time a datasource is synchronized, GRC updates fields in the row for that datasource: Last Access Synchronization Date and Last Access Synchronization Status show the date of the most recent access synchronization, and its completion status. Last Transaction Synchronization Date and Last Transaction Synchronization Status do the same for the most recent transaction synchronization or graph rebuild.

Determining Datasource IDs

When you configure a datasource, GRC assigns an ID number to it. If you intend to implement preventive analysis for an Oracle EBS or PeopleSoft datasource, you need to know its datasource ID. To determine the number, configure the datasource, then complete the following steps:

1. In the Manage Application Datasources page, select View → Columns.
2. A menu presents a list of all available columns. In it, click on Datasource ID.
3. The Manage Application Datasources page now displays a Datasource ID column. In it, note the ID number assigned to the datasource you've configured.

If, having determined the datasource IDs for your datasources, you wish to remove the Datasource ID column from view, repeat this procedure. As you do, you will notice that the Datasource ID entry in the Columns menu has a check mark; clicking on the entry removes both the check mark from the menu and the column from the page.

5

Setting Up FAACG

If you have installed Enterprise Governance, Risk and Compliance so that you can use Application Access Controls Governor to perform segregation-of-duties analysis in Oracle Fusion Applications, complete the procedures in this chapter. (If not, this chapter does not apply to you.)

As prerequisites, Fusion Human Capital Management (HCM) and Oracle Identity Manager(OIM) must be installed, through the Fusion Applications provisioning process. In conjunction with this, Oracle Internet Directory (OID) must be set up as the LDAP repository whose identity store is managed by OIM. In addition, you must have installed GRC to run with WebLogic 11g (see chapter 2 of this document).

To set up Fusion Application Access Controls Governor (FAACG), change the GRC "global user" configuration to EMAIL_AND_USERNAME (see page 4-2). Then install a "connector" within your GRC instance. (The connector collects data from a Fusion instance and provides it in a format that GRC recognizes.) Finally , use Fusion Setup Manager to perform GRC setup.

Installing the Connector

To install a connector, you use a Manage Application Libraries page available in GRC. It is assumed that you have already completed preliminary steps during installation of your earlier GRC instance — associating the GRC domain with OID, creating an OIDAuthenticator, and granting permission to the GRC code base. You need not repeat these steps for GRC 8.6.5.4000. (For detailed information about these steps, see the *Installation Guide* for GRC 8.6.5.1000.)

The Fusion connector is provided in a file called grc-connector-fusion-8.6.5.1-SNAPSHOT-connectorsetup.zip. To upload it to GRC:

1. Log on to GRC. In a web browser, enter the following URL, in which *host* is the FQDN of your GRC server, and *port* is the number you chose for the GRC managed server as you created a WebLogic domain.

   `http://host:port/grc`

2. In the Navigator, select Setup and Administration → Setup → Manage Application Libraries. Click the Connectors tab.

3. Click on Actions → Import.

4. An Import File pop-up window opens. Click on its Browse button.
5. A file-upload dialog opens. In it, navigate to, and select, grc-connector-fusion-8.6.5.1-SNAPSHOT-connectorsetup.zip, which is among the files in <grc_stage> directory (see "Downloading Files" on page 1-3). The path and name of the file then populate the field next to the Browse button in the Import File window.
6. Click on the Upload File button. A pop-up message reports the status of the upload operation. Click on its OK button to clear it, and then click on the Close button in the Import File window.
7. Log off of GRC.
8. Ensure that the following files do not exist in the library subdirectory of your web application server:
   - tika-app-0.9.jar
   - dom4j-1.6.1.jar
   - idxuserrole-1.0.jar
   - org.openliberty.arisid-1.1.jar
   - org.openliberty.arisidbeans-1.1.jar
9. Restart both the Administration Server and the GRC managed server. (Before doing so, be sure that the file tika-app-0.9.jar does not exist in the library subdirectory of your web application server).

Create and Synchronize a Datasource

Having uploaded the connector, you will need to configure a datasource that associates your Fusion instance with the connector:

1. Log on to GRC once again.
2. Navigator → Setup and Administration → Setup → Manage Application Datasources.
3. Click on Actions → Create New. A Create Datasource window opens. Enter the following values:
   - Datasource Name: Create a name for the datasource.
   - Description: Type a brief description of the datasource (optional).
   - Application Type: Select the type of business application to which you are connecting — in this case, Fusion.
   - Application Type Version: Select the version number of the Fusion instance to which you are connecting.
   - Default Datasource: Clear this check box.
   - Connector Type: For Fusion, select the Fusion connector you installed prior to working in this Manage Application Datasources page; the correct value is *FusionConnector*.
4. Click the Save or Save and Close button. A row representing the datasource appears in the Manage Application Datasources grid.

Finally, perform a data synchronization. In the Manage Application Datasources page, select the row you've just created for the Fusion datasource. Then either click on Actions → Synchronize Access, or click on the Synchronize button in the tool bar, then on a Run Now option, and then on an Access option.

Performing GRC Setup in Fusion Setup Manager

Once the Fusion connector is installed, create an implementation project for GRC in Fusion Setup Manager (FSM).

It's assumed you are familiar with use of the Fusion Setup Manager, and with terms such as *offerings*, *activities*, *tasks*, and *tasklists*. If not, see the *Oracle Fusion Application Installation Guide* and the *Fusion Setup Manager Administrator's Guide*.

Portlet Registration

Begin by ensuring that GRC is registered successfully in FSM. With FSM open, select Manage Portlet Registration under Implementations in the Tasks list (along the left of the interface). If the Manage Portlet Registration page does not show that GRC is registered, search for the "GRC Setup" Enterprise-Application and perform the portlet registration. Refer to the *FSM Administrator's Guide* for instruction on how to perform portlet registration.

Configure Offerings

Because seeded offerings are not GRC-enabled by default, use a Configure Offerings page to enable GRC for the desired offering.

1. Open the page: Select Configure Offerings under Implementations in the Tasks list.
2. Click on the Select Feature Choices icon for the selected offering. For example, selecting the icon for the Customer Data Management offering displays a screen in which Enterprise Governance, Risk and Compliance is listed.
3. Select the Enterprise Governance, Risk and Compliance entry — click on it so that a check mark appears in its check box.
4. Click Save and Close.

Implementation Project

To display a GRC-Setup screen within FSM, create one or more implementation projects. You can base a project on the offerings enabled for GRC, or you can directly add GRC-Setup tasks (and tasklists). In either case, expanding a node will display a "Go to Task" icon for the selected task within the node, and clicking on it will render the GRC-Setup screen.

Create a GRC Setup Master Record

When you select a Go-to-Task icon, a Manage Setup Configurations screen enables you to create new GRC setup records or to search for, update, or delete existing records.

Click the Create New icon to open a Configuration screen, in which you can create or register a new GRC Setup configuration master record.

In this page, supply the following values:

- Code: A code that uniquely identifies the master record being created, for example GRC_HCM.
- Name: Short name to describe the code, for example "GRC Setup Data for Human Capital Management."
- Description: Full description, for example, "This is the master record to define GRC Setup data to enforce separation of duties mandate for HCM."

Click the Save and Continue button to save the date prior to creating detail records. (Clicking on Save and Close would return you to the Manage Setup Configurations screen.)

Create a GRC Setup Detail Record

In the Configuration (master-record) screen, locate the Configuration Details panel and click on its Create New icon. A Configuration Details screen opens, in which you can create detail records for the master record.

In this page, enter the following values:

- Detail Name: Code that uniquely identifies the detail record being created.
- Name: Short name to describe the code.
- Description: Full description.
- Status: Optional field to specify the status of the detail record. It typically contains Active or Inactive.
- Services URL: http://*host*:*port*/grc/Services/GrcService, in which *host* is the FQDN of your GRC server, and *port* is the number you chose for the Administration Server as you created a WebLogic domain.
- User Name: The user name for a user granted the Admin role defined in the GRC UI.
- Password: The password for the user granted the Admin role.
- Confirm Password: The same password, entered for verification.
- GRC Data Source: The name of the datasource configured under "Create and Synchronize a Datasource" on page 5-2.

Click on Save and Close to return to the Configuration screen.

Publish Configuration

When detail records are complete, they must be published to Oracle Identity Management. From the Configuration (master-record) screen, select (click on) a detail record in the Configuration Details panel. Then select the Publish to OIM icon (it looks like an arrow pointing upwards).

A Publish Configuration to OIM pop-up window opens. In it, enter these values:

- Protocol: The protocol used for communication with the OIM managed server. Either https or t3s is recommended, but you may use any protocol the OIM managed server accepts.
- OIM Hostname: The name of the host of the OIM managed server.
- Port Number: The port of the OIM managed server.
- OIM User Name: The name of the user with admin role on the OIM managed server. (This user must be able to invoke MBean operations.)
- OIM Password: The password of the OIM user.

6

Installing PEAs

In support of the AACG preventive analysis feature, install a Preventive Enforcement Agent (PEA) on each instance of Oracle E-Business Suite or PeopleSoft that is to be subject to AACG analysis.

If a PEA for an earlier release of GRC exists on an EBS or PeopleSoft instance, you need not reinstall the PEA on that instance. If, however, you want to set up an EBS or PeopleSoft instance as an access datasource, and that instance does not have a PEA, you need to install one. See the *GRC Installation Guide* for version 8.6.5.1000 for the procedure to install a PEA.

There are distinct PEAs (and installation procedures) for EBS and PeopleSoft. See the *Oracle Enterprise Governance, Risk and Compliance Certifications Document* for supported versions of Oracle EBS and PeopleSoft.