

Oracle® Governance, Risk and Compliance

User Guide

Release 8.6.4.3000

Part No. E36191-02

September 2012

Oracle Enterprise Governance, Risk and Compliance Controls User Guide

Part No. E36191-02

Copyright © 2012 Oracle Corporation and/or its affiliates. All rights reserved.

Primary Author: David Christie

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

The software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable.

U.S. GOVERNMENT RIGHTS

Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are “commercial computer software” or “commercial technical data” pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

The software is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications which may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

The software and documentation may provide access to or information on content, products and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third party content, products and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third party content, products or services.

Contents

1 Introduction	
Suggested Limits	1-2
GRC and Language.....	1-3
Navigation	1-3
Home Page	1-4
Setting User Preferences	1-4
2 Perspective Management	
Viewing Perspective Hierarchies	2-1
Managing Perspective Hierarchies	2-2
Using the Create Hierarchy Page	2-2
Set Details.....	2-2
Create a Root Node	2-3
Create Other Nodes.....	2-3
Define the Hierarchy	2-4
Save or Submit Your Work.....	2-4
Using the Edit Perspective Hierarchy Page	2-4
3 Security Management	
Managing Roles.....	3-2
Creating Duty Roles.....	3-2
Creating Data Roles.....	3-2
Creating Job Roles and Job Duty Roles	3-4
Editing or Copying a Role	3-5

Managing Users.....	3-5
Creating User Accounts.....	3-5
Editing or Copying User Accounts.....	3-6
Unlocking User Accounts	3-7
Importing Users from an LDAP Repository.....	3-7
4 Reporting	
Running Reports	4-3
Managing Report Parameters	4-4
Reviewing Scheduled Reports	4-5
5 Application Configuration Management	
GRC Properties.....	5-1
Worklist Values	5-2
Setting Security Values.....	5-2
Analytics.....	5-3
User Integration	5-4
Configuring Notifications	5-4
Purging Incidents	5-5
6 Application Datasources and Libraries	
Configuring Datasources.....	6-1
Synchronizing Data	6-3
Uploading Business Objects	6-3
Uploading Patterns	6-4
Uploading Connectors.....	6-5
7 Other Setup Options	
Managing Lookup Tables.....	7-1
Managing Content Types	7-2
Managing Installation Options.....	7-2
Managing Assessment Results.....	7-3
Managing URL Repositories	7-3
8 Module Management	
Managing Modules.....	8-1
Configuring Module Objects.....	8-2

Managing User-Defined Attributes.....	8-3
Managing Module Perspectives.....	8-4
Data Migration	8-4
9 Jobs and Scheduling	
Managing Jobs	9-1
Managing Import and Export Jobs	9-2
Canceling a Job	9-2
Purging Job History.....	9-2
Managing Schedules	9-3
Viewing Schedules.....	9-3
Modifying Schedules	9-3
Running Jobs Manually.....	9-4

Preface

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

An Oracle Governance, Risk and Compliance (GRC) platform hosts two products — Oracle Enterprise Governance, Risk and Compliance Controls (EGRCC) and Oracle Enterprise Governance, Risk and Compliance Manager (EGRCM). EGRCC, in turn, consists of two subsidiary products, Application Access Controls Governor (AACG) and Enterprise Transaction Controls Governor (ETCG).

The GRC platform runs modules. “Financial Governance” is the name of an EGRCM module, and users may create other EGRCM modules. “Continuous Control Monitoring” (CCM) is the name of the module in which EGRCC runs. (Moreover, GRC “Tools” offer functionality used by both EGRCM and EGRCC.)

For each of EGRCM, AACG, and ETCG, a product-specific user guide addresses features particular to the product.

This *Governance, Risk and Compliance User Guide* covers most functionality common to EGRCM and EGRCC (although the *Governance, Risk and Compliance Installation Guide* covers some setup and administration topics). Refer to these guides as well as the appropriate product-specific user guide as you use a GRC product.

Additionally, implementation guides discuss concepts you should consider as you set up GRC products for use. One implementation guide exists for each of AACG, ETCG, and EGRCM, and a distinct implementation guide covers GRC security. Consult these documents as you initiate GRC processing.

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.

Introduction

Oracle Governance, Risk and Compliance (GRC) is a set of components that regulate activity in business-management applications:

- Oracle Enterprise Governance, Risk and Compliance Controls (EGRCC) comprises two elements, Application Access Controls Governor (AACG) and Enterprise Transaction Controls Governor (ETCG). These enable users to create models and controls and to run them within business applications to uncover and resolve segregation of duties violations and transaction risk.
- 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. It enables users to define risks to the company's business, controls to mitigate those risks, and other objects, such as business processes in which risks and controls apply.
- Fusion GRC Intelligence (GRCI) provides dashboards and reports that present summary and detailed views of data generated in EGRCM and EGRCC.

GRC components run as modules in a shared platform. EGRCC runs as a Continuous Control Monitoring (CCM) module. EGRCM provides a Financial Governance module by default, and users may create other EGRCM modules to address other areas of the company's business.

Because these components share a common platform, they also share some functionality. This *User Guide* documents these shared features:

- Perspective management. A perspective is a set of related values. Users can associate individual perspective values with individual objects (such as risks, models, or controls). Perspectives can serve as filtering values in reports or in the pages in which users manage objects, but they also play an important role in GRC security.
- Security management. Users are assigned job roles, which consist of duty roles and data roles. These provide a granular, flexible means of safeguarding access to GRC functionality and data.
- Reporting. Apart from the reports and dashboards provided by GRCI (if it is implemented), a Report Management option displays a variety of reports on EGRCC and EGRCM activity.

- Application setup. Although many GRC setup tasks are completed during installation, administrators can set language, security, notification, and other values at any time. (Some setup tasks, such as connecting to “datasources,” are specific to EGRCC. Others, such as creating “lookup” entries or “content types,” are specific to EGRCM. Nevertheless, these component-specific setup tasks are discussed in this *User Guide*.)
- Module management. Most module-management features pertain specifically to EGRCM, because it alone enables users to create modules other than those delivered with the product. However, aspects of module management — managing module perspectives and data migration — are common to EGRCC and EGRCM.
- Jobs and scheduling. Users can schedule and manage background tasks such as updating a “data analytics schema,” evaluating EGRCC continuous controls, exporting results, or generating reports.

Suggested Limits

GRC performs optimally if you observe the following restrictions on objects you can create. The following lists include objects discussed in this manual, as well as in user guides for Application Access Controls Governor, Enterprise Transaction Controls Governor, and Enterprise Governance, Risk and Compliance Manager.

In GRC as a whole, the following are suggested maximum amounts:

- Perspectives: Fifteen per application, of which no more than five are for security (excluding system perspectives).
- Perspective depth: Eight levels.
- Perspective nodes: Ten thousand.
- Perspective Nodes per record: Fifteen
- Attachment size: Ten megabytes. (Attachments are files that may be associated with perspectives, EGRCC incidents, and EGRCM objects.)
- Description field length: Ten thousand characters.

In EGRCM, the following are suggested maximum amounts:

- Custom modules: Three.
- User defined attributes: Twenty per module object.

In EGRCC, the following are suggested maximum amounts:

- Entitlements per control: Two (AACG).
- Access points per entitlement: Fifteen (AACG).
- Business objects per control: Five (ETCG).
- Global path conditions per datasource: Thirty (AACG).
- CCM Result Management page: Optimize for 10,000 or fewer rows.
- Datasources per control: Two.

GRC and Language

Enterprise Governance, Risk and Compliance can display information in any of twelve languages: US English, traditional Chinese, standard (simplified) Chinese, Danish, Dutch, French, German, Italian, Japanese, Korean, Brazilian Portuguese, or Spanish. An administrator uses the Manage Application Configurations page to make a selection of these languages available to users (see page 5-1).

For each individual user, GRC “selects” the language chosen for the user when his GRC user account is created (see page 3-5), or updated by him in his user profile (see page 1-4).

EGRCC may connect to any number of datasources (see page 6-1). Each may use a language distinct from the others. For that matter, a given datasource may incorporate more than one language. To display information from such varying datasources, GRC follows these rules:

- Prompts (field names, button names, navigation links, and so forth) appear in the language selected for GRC (through the process described above).
- Generally, EGRCC presents processing results only in the selected language; any results in other languages are omitted. (“Processing results” are values entered to define AACG or ETCG models and controls, AACG entitlements and conditions, and so forth, as well as results returned when those objects are evaluated.)

Thus, for example, if a user logged on in French, and the instance were connected to a single, French-language datasource, it would display all results properly. If it were connected to a second, German-language datasource, it would display the processing results stored on that datasource only if the user logged off and logged back on in German (in which case, it would cease displaying the French results).

Further, a single datasource may itself use more than one language. If so, EGRCC would display processing results in its selected language, but filter out results in other languages on that single datasource. If, for example, a user logged on in French, and the instance were connected to a datasource that defined AACG controls in both French and German, it would display the French controls (and the incidents generated by them), but omit the German controls (and their incidents).

There are exceptions to that second rule. Some of the elements you can configure for AACG are “global” — they apply not to individual controls, but to all entities configured for a given datasource. For example, “global conditions” define exemptions from all the controls on a datasource. In such a case, GRC presents values in the language of the datasource, no matter what language is selected, and even though mixed languages may appear on screen.

Navigation

Click on a Navigator link near the upper left of any GRC page to display links to work areas you can use. The links you see depend on the rights granted to you by your roles. A Tools list provides access to features shared by EGRCC and EGRCCM, and features in this list are the focus of this *User Guide*.

(Additionally, a Financial Governance list offers links to pages in which users can manage objects within that EGRCM module; a comparable list appears for each custom EGRCM module. A Continuous Monitoring list offers links to EGRCC features.)

If the Navigator contains three or fewer modules, the links you can select are visible; simply click on one to navigate to a feature you want to use. If the Navigator contains four or more modules, they are “collapsed”; only the module names are visible. Click on the icon next to a module name to display its links (and then click on a link to navigate to a feature you want to use)

Home Page

Your home page (the one that opens when you log on to GRC) contains several listings of tasks that await your attention — worklists, notifications, and a watchlist.

- A worklist is both a record of a task that has been assigned to you and a link to the GRC page on which you can complete the task.

To view your worklists, select the Worklists tab in the Pending Activities area of your home page. You can search for worklist entries. Each of the standard search fields assumes a “Starts With” operator — the search returns all values starting with the text you enter. You can select an Advanced search to use other search operators.

- A notification is a record of a task in which you have an interest, but for which no action is required from you. Like a worklist, a notification is also a link to the page on which the task has been undertaken. To view your notifications, select the Notifications tab in the Pending Activities area of your home page or any object overview page. You can search for notifications in the same way you search for worklists.
- The watchlist is a summary of your worklist entries, categorized by module and, within each module, by activity type. You can expand or collapse sets of watchlist entries so that you can focus only on a particular set. The watchlist appears near the upper left corner of your home page.

If your EGRCM instance includes Oracle Fusion GRC Intelligence (GRCI), and if your roles give you access to GRCI, your home page also includes an Intelligence tab. Click on it to view GRCI dashboards and reports.

To return to the home page from any other page in EGRCM, click on the Home link near the upper right of any page.

Setting User Preferences

From any page in GRC, the user who is currently logged on can open User Preferences, review information pertaining to his own user account, and change some of it.

To open User Preferences, click on the Preferences link near the upper-right corner of any GRC page. A User Preferences dialog appears, divided into three sections:

- A Details section displays your username and status as read-only values. It also provides write-enabled fields in which you can modify your first, middle, and last names, email address, password, and tracking information — a second email address, office and mobile phone numbers, physical address, and position and organization.
- Email Address 1 is the address to which EGRCM sends worklist advisories (if notifications are enabled under Manage Application Configurations in the Setup and Administration tasks). A password is case-sensitive and must consist of at least eight characters, taken from each of four character sets: uppercase letters, lowercase letters, numbers, and special characters, which comprise !@\$%&*. A password is invalid if it matches or contains the username, and it must not match any of the previous three passwords.
- In a Regional section, select the territory in which you work and related information: a time zone, a language in which GRC presents information, and date, time, and number formats appropriate to that language. You can choose among languages configured for use in the Properties tab of the Manage Application Configurations page.
- In the Assigned Roles section, view a list of roles assigned to you. You cannot change these.

When you finish setting user-profile options, save them: Click on the Save button or the Save and Close button.

Perspective Management

A perspective defines a context in which objects exist. That context may be organization, region, regulatory code, or any other concept the company determines to be meaningful. Each perspective is a set of related values. The values are hierarchical — they have parent/child relationships to one another. Users associate individual values with individual objects, in effect cataloging them. In EGRCM, these objects include processes, other base objects, risks, and controls. In EGRCC, they include models, continuous controls, and incidents.

For example, an Organization perspective might contain values that map the structure of your company. Divisions, for instance, might be immediate children of the organization; each division might be the parent of a set of operating units; and so on. This would enable users to associate individual risks, controls, or other objects with the divisions, units, or other corporate entities to which they apply.

Perspectives also play a part in GRC security. Users are assigned job roles, which contain duty roles that define functionality available to users, and data roles that define sets of data available to users. A data role may be associated with a perspective value, and if so would grant access only to data concerning objects associated with that perspective value. To use the Organization example, a data role might be associated with the perspective value for a specific operating unit within a particular division. That role would grant access only to data pertaining to that operating unit.

In EGRCC, perspectives also help determine which users resolve incidents generated by continuous controls. As a continuous control is created, perspective values are assigned to it. A user can review its incidents if his job role contains a data role associated with perspective values that match values assigned to the control. (The job role would also need to contain a duty role with the privilege for incident review.)

To work with perspectives, select Perspective Management under Tools in the Navigator.

Viewing Perspective Hierarchies

In the Manage Perspective Hierarchies page, the panel labeled “Search Results: Perspective Hierarchies” displays a list of perspective hierarchies configured for your GRC instance (or a set of those hierarchies that conform to search criteria entered in the “Search Perspective Hierarchies” panel). The list displays summary information — for each hierarchy, the name, description, status, and current state.

Click on the name of a hierarchy to open a Manage Perspective Hierarchy page specific to the hierarchy you've selected:

- A Definition panel displays its name, type, description, current status and state, the date of its most recent revision and its revision number, the names of users who created and most recently updated it, and the dates on which they did so.
- A Hierarchy Details panel displays the values selected for the perspective, as nodes in a hierarchical "tree." Click on Assessments tab or the Issues tab to see records of assessments conducted of the hierarchy as a whole, or issues raised against it.
- Click on any of the nodes in the hierarchy, and an Item Details panel displays general details of its configuration, and records of its assessments, issues, and components (if any) related to it.

Click the Done button to return to the home Manage Perspective Hierarchies page.

Managing Perspective Hierarchies

From the home Manage Perspective Hierarchies page, you can:

- Choose to create a perspective hierarchy. Select Create Perspective Hierarchy in the Tasks panel. Or, in the Search Results panel, select Actions > Create. Any of these actions opens a Create Perspective Hierarchy page (see below).

(Once created, a perspective must be associated with the types of object with which it is to be used. This is done through Manage Module Perspectives. See page 8-4.)

- Choose to edit a hierarchy. Click in the Search Results panel on the row for the hierarchy you want to edit. Then click on Actions > Edit. This opens an Edit Perspective Hierarchy page (see page 2-4).
- Delete a perspective hierarchy. Click in the Search Results panel on the row for the hierarchy you want to delete. Then click on Actions > Delete. Respond to a pop-up message that asks you to confirm the deletion.

Using the Create Hierarchy Page

To create a perspective hierarchy, open the Create Perspective Hierarchy page (see above). Then (as described below) define its details, create a root node, create other nodes, arrange all nodes into a hierarchy, and save your work.

Set Details

First, enter values in a Details panel: Name and Type are required. Also select a status (Active or Inactive) for the hierarchy as a whole, and optionally write a description of the hierarchy.

You may select a given Type value for any number of hierarchies, but all values (nodes) for a given type must be unique — hierarchies of a given type may not share values. A given value may be used in more than one hierarchy only if the hierarchies are of different types. (Values available in the Type LOV are created at the Manage Lookups page, available in the Setup and Administration tasks. If no existing type is appropriate for the perspective you are creating, have a new type created in the Manage Lookups page.)

If you have created user-defined attributes for the Perspective object, fields for those attributes appear in an Additional Details panel. To reach it use the scroll bar to the right of the Details panel, and enter appropriate values.

Create a Root Node

Second, create a root node:

1. In the Hierarchy panel, select Actions > Create. A Create Perspective pop-up window opens.
2. In the Name field, enter a name for the node. (You may choose to give the root node the same name as that of the perspective hierarchy, although this is not necessary). Note that a Type value matches the Type selection you made in the Details panel, and cannot be changed.
3. Optionally, describe the node in the Description field.
4. If user-defined attributes have been created for the perspective object, fields representing these UDAs appear in an Additional Details panel. Provide values for these fields.
5. Optionally, specify any number of attachments — for example, a text file that provides more information about the node than can be contained in the Description field.
 - a. Click on the green plus sign next to the Attachment label. An Attachments pop-up opens.
 - b. Select Actions > Add. A new row appears.
 - c. Select a Type (desktop file or url), and click the Browse button to navigate to, and select, the attachment you want. Select a content type and compose a title and, optionally, a description.
 - d. To create additional attachments, repeat steps b and c for each attachment.
 - e. Click the OK button to return to the Create Perspective pop-up.
(You can also delete an attachment by opening the Attachments pop-up, selecting a row, and selecting Actions > Delete.)
6. Select a status for the node — typically Active.
7. Select the Save button to save the node and return to the Create Perspective Hierarchy page.

Create Other Nodes

Third, populate the Hierarchy panel with nodes representing all the remaining values you want the perspective to contain. By default, these nodes are indented one level to the right of the root node, indicating they are children of it. To create these child nodes, use the same process as you used for the root node (above).

You can also edit nodes. Click on a node, then select Actions > Edit to open an Edit Perspective pop-up; modify any of the values initially set for the node; then click the Save button. Although you cannot delete a node, you can set its status to Inactive as you edit it.

Define the Hierarchy

Fourth, adjust the relative positions of nodes to define their hierarchical relationship to one another. A parent node is situated above and to the left of a child node; nodes are peers if they are indented equally; a child node is situated below and to the right of its parent. To adjust the position of a node, click on it. Then:

- Select Actions > Decrease Indent to move the node to the left.
- Select Actions > Increase Indent to move the node to the right.
- Select Actions > Move Up to move the node up.
- Select Actions > Move Down to move the node down.

For ease of viewing, you can cause the Hierarchy panel to display only a node (at any level of the hierarchy) and those that descend from it. To do so, click on a node, then select View > Show as Top. To restore the display, select View > Go Up to display nodes one level higher, or View > Go to Top to display the entire hierarchy.

Click on any of the nodes in the hierarchy, and an Item Details panel displays tabs in which you can view general details of its configuration, assessments and issues concerning it, and its related components (the objects with which the node has been associated). You can use this display to add attachments (see page 2-3) to a node, but otherwise it is read-only.

Save or Submit Your Work

Finally, save or submit the perspective hierarchy. Typically, you save the hierarchy if you intend to work on it further before making it available to others, or submit it when it is ready for use by others. If, for example, your workflow calls for review and approval of perspective hierarchies, submitting the hierarchy would place it in a state that makes it available for review or approval. It is assumed that although you may choose at first to save a hierarchy, your final action will be to submit it so that it is active in your system.

To save a perspective hierarchy, click on the Save button, which causes the hierarchy to reopen in the Edit Perspective Hierarchy page. Or, click the Save and Close button (available in a drop-down field available from the Save button); this restores the home Manage Perspective Hierarchies page. To submit the hierarchy, click the Submit button.

Using the Edit Perspective Hierarchy Page

To edit a hierarchy, open it in the Edit Perspective Hierarchy page. (See “Managing Perspective Hierarchies” on page 2-2.) It’s laid out similarly to the Create Perspective Hierarchy page, and in general you can modify perspective values in the same way as you create them.

However, some elements of a perspective hierarchy cannot be changed — for example, its name and type. Your ability to change other elements may depend upon the state of the hierarchy. For example, if a perspective hierarchy is in a review or approval workflow, the edit action is disabled. Therefore you may discover, as you work in the Edit Perspective Hierarchy page, that some values are read-only.

Security Management

GRC assigns individual users distinct combinations of rights to data and to functionality. To define access to functionality, it uses these components:

- A “privilege” is a specific feature GRC can make available to users.
- A “duty role” is a set of privileges. Each duty role defines one or more tasks a user can complete in GRC — for example creating controls, or approving changes to them.
- A “job duty role” is a set of duty roles. It encompasses the functionality a user needs to do a large-scale job such as Control Manager or Risk Manager.

To define access to data, GRC uses these components:

- A “primary data role” defines a narrowly focused set of data. Each primary data role sets at least three conditions: data must belong to a specified module; exist at one or more specified states; and be subject to specified actions.

If a primary data role supports assessment activities in EGRCCM, it sets a fourth condition: data must be associated with a specified value for a seeded perspective called Activity Type.

If a primary data role supports work with models, continuous controls, or incident results in EGRCC, it sets a fourth condition: data must be associated with a value for a seeded CCM Type perspective, which distinguishes between data for use by AACG and data for use by ETCG.

- A “composite data role” is a set of primary data roles. It defines the data to which a user can apply the functionality granted in a job duty role. Users may create “custom perspective data roles,” each of which combines a composite data role with a filter that allows access only to data associated with a specified perspective value.

To combine functionality and data access, GRC uses these components:

- A “job role” comprises a job duty role and a composite data role (or custom perspective data role).
- Each GRC user is assigned one or more job roles.

As you configure GRC security, consult not only this chapter, but also the *Oracle Governance, Risk and Compliance Security Implementation Guide*.

Managing Roles

From a Manage Roles page, you can create duty roles, all types of data roles, and job duty and job roles. You can also edit and copy roles. To open the Manage Roles page, select Setup and Administration under Tools in the Navigator, then Manage Roles under Security.

GRC includes a large number of job, duty, and data roles that support the Financial Governance and CCM modules. Create new roles only if delivered roles do not meet your needs. (For example, if you create new modules, create new roles to support those modules.)

To view any type of role, select it in the Roles panel of the Manage Roles page. Use query by example to search for the role by any combination of name, description, type, status, or update date. Click on the row in which the role appears, and the logic by which the role defines functionality or data access appears in the Role Logic panel. Or, click on the name of a role to open a View page that provides full details of the role configuration.

Creating Duty Roles

To create a duty role:

1. In the Manage Roles page, select Actions > Create Duty Role. A Create Duty Role page opens.
2. In the Details panel, enter a name and, optionally, description of the role. Select a status — Active or Inactive.
3. In the Selected Privileges panel, choose privileges for the role.
 - To add privileges, click on Actions > Select Privileges. A Privileges pop-up window opens; in it, select any number of privileges. (You can enter values in search fields to search for privileges by name, navigator entry, or activity.) Then click on the OK button.
 - To remove privileges, select any number of them in the Selected Privileges panel. Then click on Actions > Delete.

In either case, to select a single privilege, click on it. To select a continuous set of privileges, click on the first, press the Shift key, and click on the last. To select a discontinuous set, press the Ctrl key as you click on privileges.

4. Save the role: Click the Save button or Save and Close button.

Creating Data Roles

A data role (of any sort) consists of filters that select the data to which the role grants access. Each filter expresses a relationship between an attribute and a value — for example that module (the attribute) equals Financial Governance (the value). Depending on further configuration, the role would include or exclude data belonging to the item that satisfied the defined relationship (in this example, the Financial Governance module).

- A primary data role contains at least three filters. One specifies a module that the role is to support. The second specifies one or more states in which data must

exist for the role to grant access to it. (For a list of states, see “State Action” in the *GRC Security Implementation Guide*.) The third specifies an action that may be performed on data at the selected state.

If the role supports EGRCC assessment activities, a fourth filter selects a value for a seeded Activity Type perspective, which limits the role to data needed for a particular type of assessment. If the role supports work with EGRCC models, continuous controls, or incident results, a fourth filter selects a value for a seeded CCM Type perspective — Access or Transaction — which limits the role to data used in access analysis or in transaction analysis.

(A complete set of primary data roles is seeded with GRC. Because you can reference these, you may have no need to create a primary data role.)

- A composite data role consists of filters, each of which selects a data role. The composite role grants access to all the data defined by its data roles.
- A custom perspective data role contains one or more filters that select composite data roles and one or more filters that select perspective values. The role limits the access granted by the composite roles to data associated with the perspective values.

In particular, EGRCC roles may contain filters that select perspective values representing datasources and business objects to which the role grants access. (A datasource is the database of a business application subject to EGRCC models and controls; a business object is a set of conceptually related data points. Each has its own perspective hierarchy, which is updated automatically as new datasources are configured or business objects are added.)

A role that supports work with controls, models, entitlements, or global conditions must include a datasource filter and a business object filter. A role that supports work with incidents, access requests, or path conditions must include a datasource filter (but not a business object filter). A given data role must contain no more than one filter for datasource and one filter for business object, although each of these filters can name any number of datasources or business objects.

To create any sort of data role:

1. In the Manage Roles page, select Actions > Create Data Role. A Create Data Role page opens.
2. In the Details panel, enter a name and, optionally, description of the role. Select a status — Active or Inactive.
3. In the Filters panel, click the green plus sign. A new row appears, in which a filter is to be defined. In its Filter Name field, type a name for the filter.
4. In the Object field, select Perspectives if the filter is to designate a perspective value (for a primary data role or custom perspective data role). Select Data Attributes for any other type of filter.
5. If you selected Data Attributes in the Object field, use the Attribute field to select a value appropriate for the filter you are creating: Module, State, or StateAction (for a primary data role), or DataRole (for a composite data role or custom perspective data role). If you selected Perspectives in the Object field, select the name of a perspective hierarchy in the Attribute field.

6. If you selected Data Attributes in the Object field, select Equals or Not Equals in the Condition field. If you selected Perspectives in the Object field, select Equals, Not Equals, or Includes Children in the Condition field.
7. In the Values field, click on a button that looks like a magnifying glass. A pop-up window opens; in it, select a value that completes the relationship definition already begun in the Attribute and Condition fields.

For example, if your attribute is Module and your condition is Not Equals, your value will be the name of a specific module; this would designate data belonging to all modules other than the one you've named.

Or, if your attribute is the Activity Type perspective and your condition is Equals, the value may be the name of a node in the Activity Type hierarchy (for example, Certification); this would designate data associated with that node. Or, if the condition is Includes Children, the filter would designate data associated with the node you select and all its child nodes.
8. In the Include/Exclude list box, select Include to allow access to the data you've defined, or Exclude to prevent access to that data.
9. Repeat steps 3–8 for each remaining filter the role requires.
10. Only if necessary (if, for example, you determine a filter is unnecessary), delete filters. Select one or more in the Filters panel and click the red × icon.
11. When you are satisfied with the filters you've configured, click on the Save or Save and Close button.

Creating Job Roles and Job Duty Roles

A job duty role consists of two or more duty roles, combining the functional access granted by those duty roles. A job role combines a job duty role with a data role (typically a composite data role or a custom perspective data role) to associate a set of functionality with the data to which it applies. In either case:

1. In the Manage Roles page, select Actions > Create Job Role. A Create Job Role page opens.
2. In the Details panel, enter a name and, optionally, description of the role. Select a status — Active or Inactive.
3. In the Selected Roles panel, chose subordinate roles for the role you are creating:
 - To add roles, click on Actions > Select Roles. An Add Role pop-up window opens; select any number of roles. (You can enter values in search fields to search for roles by name, description, or type.) Then click on the OK button.
 - To remove roles, select any number of them in the Selected Roles panel. Then click on Actions > Delete.

In either case, to select a single role, click on it. To select a continuous set of roles, click on the first, press the Shift key, and click on the last. To select a discontinuous set, press the Ctrl key as you click on roles.

4. Click the Save button or the Save and Close button.

Editing or Copying a Role

To edit a role, select its row in the Roles panel of the Manage Roles page, then select Actions > Edit. The role opens in an Edit page, in which you can modify the role in much the same way as you would create it.

You can copy a role, to use it as the basis for a new role. Select its row in the Roles panel of the Manage Roles page, then select Actions > Copy. The Create Role page opens, populated with all the information (except name) from the selected role. Fill in a new name, then modify data from the copied role as needed.

Managing Users

A Manage Users page provides information, in read-only format, about GRC user accounts. To open the Manage Users page, select Setup and Administration in the Navigator, then Manage Users under Security.

Its upper panel, labeled Manage Users, displays a list of existing user accounts, together with summary information about each — the username (by which the user identifies herself as she logs on); the user's given name, surname, and email address; the user's status; and the date and time at which the account was last updated.

In the Manage Users panel, select (click on) the row for a user whose information you wish to review. A lower panel, labeled User Roles, lists the job roles assigned to the user (together with a description and status for each role).

Alternatively, click on a user's username, and a View User page opens, providing full details for the user, with a list of roles the user has been assigned. From this page, you can select an option to edit the user account. (Otherwise, select a Cancel button to return to the Manage Users page.)

You can use options available from the Manage Users page to create, edit or copy, or unlock user accounts, or import them from an LDAP repository.

Creating User Accounts

To create a user account:

1. In the Manage Users page, click on Actions > Create User. A Create User page opens.
2. Enter values in the Details section of the Create User page. To do so, click in each field (or press the Tab key to move from an active field to the next field).
 - In the Username field, type a name by which the user identifies herself as she logs on. A username consists of alphanumeric characters, may be any length, and is case-sensitive.
 - In the Last Name, First Name, and Middle Name fields, enter the user's surname, given name, and middle name. (The middle name is optional.)
 - In the Email Address 1 field, supply an email address for the user. GRC uses this address to alert the user of worklist tasks for review.
 - Optionally, provide tracking information in the appropriate fields — a second email address, office and mobile phone numbers, physical address, and the user's position and organization.

- In the Status field, select a status for the user — typically Active. Select Inactive if a user is no longer eligible to use GRC. You can select Locked, although typically this status is set automatically by GRC if the user fails to log on properly after a number of attempts specified in the Manage Application Configurations page. (See “Unlocking User Accounts,” page 3-7.)
 - In the Language field, select a language in which GRC displays information when the user logs on. In a Manage Application Configurations page, an administrator has selected languages from a set of twelve. This field enables you to choose one language from among that administrator’s selection. (The user can reset this value while configuring a user profile.)
 - In the Password field, type a password with which the user validates her username as she logs on. Retype the password in the Confirm Password field. A password is case-sensitive and must consist of at least eight characters, taken from each of four character sets: uppercase letters, lowercase letters, numbers, and special characters, which comprise !@#%&*. Moreover, the password is invalid if it matches or contains the username.
 - A Source value is updated by GRC. It reads *Internal* if the user account was created in GRC, or *LDAP* if it originated in a database that uses LDAP technology to share user information. An LDAP user becomes an internal user when he is assigned an GRC role; at that point, his Source entry changes to *Internal*.
3. Assign job roles to the user:
- To add roles, click on Action > Select Roles in the Selected Roles section of the Create User page. An Add Role pop-up window opens. In it, select one or more roles (use the Shift or Ctrl key to select a continuous or discontinuous set of roles). Then click the OK button.
 - To remove roles, select one or more in the Selected Roles section of the Create User page. (Again, use the Shift or Ctrl key to select a continuous or discontinuous set of roles.) Then click on Action > Delete.
4. Save the user account. Click on the Save button to save the account and reopen it in an Edit User page. Or, click a Save and Close button to save the account and return to the Manage Users page. (Alternatively, click a Cancel button to return to the Manage Users page without saving the values you’ve configured.)

Editing or Copying User Accounts

Select a user account to edit in either of two ways:

- In the Manage Users page, click on the row for the user account you want to edit. Then click on Actions > Edit User.
- In the Manage Users page, click on the username for the user account you want to edit. The View User page opens; in it, click on the Edit button.

An Edit User page opens, displaying values already configured for the user whose account you want to edit. Using the procedures described for creating a user, modify the Details settings, Selected Roles settings, or both for the user.

You cannot, however, edit the Username field. To change a username, set the existing account to the Inactive status, and create a new account.

You can copy an existing user account as a template for a new account. In the Manage Users page, select the row for the existing account, then select Actions > Copy User. The Create User page opens; its Details panel displays the source user's last name, first name, and status, but other fields are blank; its selected roles panel displays the source user's roles. Edit these values and supply required values to create a new user account.

Unlocking User Accounts

If a user fails to log on after a number of attempts specified in the Manage Application Configurations page, GRC automatically locks his account. In that case, no one is able to log on to the account, and its status field is set to Locked. To unlock the account, edit it, resetting its status field to Active. The account is then usable once again.

Importing Users from an LDAP Repository

You can import users from an LDAP repository as GRC users. You must first configure LDAP in the User Integration tab of the Manage Application Configurations page. Once that's done, complete this procedure:

1. From the Navigator, choose Setup and Administration.
2. In the Security tasks list, choose Manage Users.
3. In the Manage Users page, select Actions > Import from LDAP.
4. An Import from LDAP pop-up window lists users. Put a check mark (click) in the Select field for each user you want to import.

Only active LDAP users who are not already created as EGRCM users are listed. If an LDAP user has the same username as an existing EGRCM user, you will not be able to import that LDAP user.

5. Click on the OK button to close the pop-up window and import the selected users.

Users imported from LDAP are at Active status, and the source field displays *LDAP*. No roles are assigned to them; roles must be assigned manually.

Reporting

From a Report Management page, you can run ad hoc reports or schedule them to be run at intervals over a period that you define. The Report Management page saves the scheduled reports it generates, enabling you to view them at any time. To open the page, select Report Management in the Tools section of the Navigator.

Then, under Report Management in the Tasks panel, select the type of report you want to run. The selection available to you depends on whether you use EGRCM, EGRCC, or both (and on the access granted to you by your data roles).

CCM Control Management reports include the following:

- The Control Detail Extract Report provides information about continuous controls. For each control, it gives the processing logic, conditions, and other values that define it; users who created or updated it, and when they did so; and perspectives and result investigators associated with it.
- The Conditions Report provides information about three sorts of condition that may be set in AACG: A global condition specifies objects exempted from controls on a given datasource; the report lists global conditions by datasource. A global path condition excludes one access point from another, exempting paths including both points from analysis; the report identifies each excluded access point and its parent. A control-specific condition is like a global condition, but applies to only one control; the report lists controls that contain conditions.
- The Entitlement Report lists access points belonging to each in a set of entitlements (an entitlement being a set of access points that may be included in a model or continuous control).

CCM Result Management reports include the following:

- The Access Approvals report displays records of role assignments in business-management applications which, because they violated Approval Required controls, were suspended until a control participant could review them.
- The Result Summary Extract Report lists incidents generated by access and transaction controls, providing summary details for each. These include an “Incident Information” value — the path by which a user can reach one in a conflicting pair of access points, or the value of the first attribute selected (during model configuration) to characterize a suspect transaction.

- The Access Incident Details Extract Report lists incidents generated by access controls, providing not only the information that would be included in the Result Summary Extract Report, but also additional details.
- The Transaction Incident Details Extract Report lists incidents generated by a transaction control. It provides not only the information that would be included in the Result Summary Extract Report, but also values for all attributes selected to characterize suspect transactions. These attributes vary from one control to another, so each run of the report must focus on a single control.
- The Access Point Report lists paths to access points involved in conflicts. Each record in the report is not a conflict in itself, but rather one path (potentially among many) to one of the access points involved in a conflict.
- The Access Violations by User Report lists ten users with the greatest number of conflicts, the number of conflicts for each, and information about those conflicts.
- The Access Violations Within a Single Role (Intra-Role) Report lists roles for which access controls generate conflicts between privileges granted within a role, so that the role cannot be assigned to any user without a conflict occurring.
- The Intra-Role Violations by Control Report lists access controls that generate intra-role conflicts for which incidents exist at the Assigned, Remediate, Authorized, or Accepted status. For each control, it also lists the roles for which the conflicts are generated.
- The Global Users Report provides information about global users — IDs created by EGRCC, each of which identifies one person, and correlates to any number of potentially varying IDs that person may have in business applications subject to access controls.
- The Result by Control Summary Extract Report lists access and transaction controls that have generated pending incidents, and provides information about each control.
- The Users with Access Violations by Control Report lists access controls that have generated incidents at the Assigned, Remediate, Authorized, or Accepted status. For each control, it lists users whose work assignments have violated the control.

GRCM Assessment Management reports include the following:

- The Assessment Details Report displays information about assessments conducted against selected objects.
- The Control Assessment Extract Report is an Excel report that lists controls and their related assessment activities.
- The Control Assessment Report is a PDF report that lists controls and their related assessment activities.

GRCM Control Management includes a single report: The GRCM Control Details Report provides information about GRCM controls. For each control, it gives the name, description and other values that define it, the users who created or updated it, and when they did so.

GRCM Issue Management reports include the following:

- The Issue Details Report provides information about selected issues, including the object against which the issue is raised, issue status and state, users who created or updated it, and when they did so, and other values.
- The Issue Listing Extract provides information similar to that of the Issue Details Report, for analysis in Excel.

GRCM Risk Management reports include the following:

- The Risk Control Matrix Report lists risks, controls, or processes and related information (perspectives, UDAs, and other values).
- The Risk Control Matrix Extract provides information similar to that of the Risk Control Matrix Report, for analysis in Excel.

GRC Administration reports include the following:

- The Change History Report displays the change history for selected objects.
- The Pending Activity Report displays the outstanding worklist items by user.
- The Related Objects Report displays objects related to each of a specified type of object.
- The Worklist Items Requiring Reassignment Report lists worklist items that cannot be completed as currently assigned.

GRC Security reports include the following:

- The Inaccessible Records Report lists data records that cannot be accessed by any user, owing to how GRC security is defined.
- The Record Assignment Report displays job roles, users who have specific job roles, and what access they have to objects.
- The Role Assignment Report displays the roles that each user has with GRC. You can enter a job role, and the report displays users assigned that role.
- The Unassigned Perspective Values displays perspective values with related objects, for which no job role has the correct privileges.

Running Reports

Once you've selected a category of reports from the Tasks panel for the Report Management page, the upper panel of the page lists a set of reports.

1. Click in the row for the report you want to run.
2. Click on Actions > Run Now or Actions > Schedule.
3. A Parameters pop-up window opens. In it, select parameter values. (See "Managing Report Parameters" on page 4-4).
4. If you selected Run Now in step 2, the Parameters window displays a Generate Report button. Click on it to generate the report.

If you selected Schedule in step 2, this button is replaced by a Schedule Information button. Click on this button to produce a Schedule Parameter pop-

up window. Enter values that set a name for a schedule, the date and time at which it should start, the regularity with which the report should run, and the date and time (if any) on which the schedule should expire. Then click on the Schedule button.

Managing Report Parameters

As you run reports you can select parameter values, thus focusing the results on records that match those values. Parameters vary from one report to another; in general, they correspond to the selections you make as you create or otherwise work with the object on which you are reporting. As you set parameters, you would select among the same values.

For example, a Control Detail Extract Report (for EGRCC) enables you to select among values you would set as you create continuous controls, such as name, type, enforcement type, priority, and other values. For each report, you can also select the format in which the report should be generated — PDF (Adobe Acrobat file) or CSV (a text file for export to another application, such as a spreadsheet).

Select parameter values in a Parameters pop-up window that opens as you run or schedule reports. (See steps 2 and 3 of “Running Reports“ on page 4-3.)

You can save sets of parameter values for each report, so that you can select them easily as you run reports:

1. In the Parameters window that opens when you select the Run Now option in the Report Management page, select a set of parameter values. Then click the Save Report Parameters button.
2. A Create Saved Report Parameters dialog opens. In it, create a name for the set of parameter values, and click the OK button.

To use a set of saved parameter values, choose it in the Select Saved Report Parameters list box that appears in the Parameters pop-up window. (This list box is available regardless of whether you are running an ad hoc report or scheduling a report.)

In this list box, you can select a Personalize option. This opens a Personalize Saved Report Parameters dialog. In its list box, select one of the sets of saved parameters. Then do any of the following:

- Click the Delete button to delete the set of saved parameters.
- Select or clear a Show in Saved Report Parameters check box to make the set of parameters available, or hide it, in the Select Saved Report Parameters list box.
- Select or clear a Default Report Parameter check box to apply the set of parameters each time you run the report. (This option should be selected for only one set of parameters per report. Clear the existing selection before setting this option for a new set of parameters.)

Select the Apply button in the Personalize Saved Report Parameters dialog to implement your selections, and the OK button to close the dialog.

Reviewing Scheduled Reports

If you have scheduled a report to run, the bottom portion of the Report Management page can display either a row for each generation of the report or a row for each schedule configured for the report. (Note that the Last Run Date and Last Run By columns in the top portion of the screen are populated by GRC, but only for scheduled runs of reports, not for ad hoc runs.)

To view a report generated on a schedule:

1. In the top portion of the Report Management page, click on the title of the report you want to see.
2. In the top portion of the page, click on Display > Report History.
3. In the bottom portion of the Report Management page, click on the row representing the instance of the report you want to see. Then select Actions > View Report.

(To remove an instance of a report, click on its row in the bottom portion of the page, and then select Actions > Delete.)

To view or modify the schedule on which the report was generated:

1. In the top portion of the Report Management page, click on the title of the report whose schedule you want to see.
2. In the top portion of the page, click on Display > Scheduled Reports.
3. In the bottom portion of the Report Management page, each row represents a current schedule. (Schedules that have reached their end dates are removed from the list.) Click in the row for a schedule, then select Actions > Reschedule/Unschedule Report Job. The Schedule Parameter pop-up window reopens. You can re-enter schedule values and select a Reschedule button, or turn off the scheduling by selecting an Unschedule button.

Application Configuration Management

The Manage Application Configurations page is divided into tabs, in each of which you can set options that determine how GRC works. In pages opened from some tabs (as noted below), some values are entered during installation and are not expected to be changed subsequently. You may choose to modify other settings from time to time.

To open the Manage Application Configurations page, select Setup and Administration under Tools in the Navigator, then Manage Application Configuration under Setup.

GRC Properties

The Properties tab opens a page in which you can set values required for GRC to connect to its database. You can also select performance and language options, and download or upload a GRC database schema.

Fields in the Installation Configuration section of the Properties page record database connection settings. Fields in the Performance Configuration section record settings that may optimize GRC performance. Typically, fields in both sections are completed during GRC installation and are not changed subsequently. For more information on values appropriate for these fields, see the *Governance, Risk and Compliance Installation Guide*.

In the Language Preferences section, choose languages in which GRC users may work. Select their check boxes, then select Actions > Save. Once selected here, languages are available to administrators as they create GRC user accounts, or to GRC users as they set user preferences.

Use the Schema Import Export section to download the GRC database schema to a file, or to upload a copied schema from a file. A download copies the schema whose settings are recorded in the Installation Configuration fields. For a schema file to be uploaded, an empty schema must be created to accept the contents of the file (and a tablespace must be created for that schema). Moreover, before the Schema Import Export fields have any effect, you must complete a setup procedure. This setup is typically performed during installation; for more information about it, see the *Governance, Risk and Compliance Installation Guide*.

In a typical operation, a GRC instance is used for a time, and so its schema contains operational data. That schema and its data are to be copied for use with a second GRC instance.

- In the database server, an administrator creates an empty schema, and a tablespace for it. (For information on creating a GRC schema and tablespace, see the *Governance, Risk and Compliance Installation Guide*.)
- From the first GRC instance, a user downloads the GRC schema to a file.
- From that same GRC instance, the user uploads the file content to the newly created, empty schema.
- Finally, the user installs a second GRC instance (or opens an existing instance). In that second instance, he opens the Manage Application Configurations page, selects the Properties tab, and uses the Installation Configuration fields to enter connectivity values for the schema copy.

To download a schema:

1. In fields next to the Download button, enter the username and password for the GRC schema whose connectivity settings are recorded in the Installation Configuration fields.
2. Click the Download button.
3. An Export File dialog opens. Navigate to a directory in which you want to save the download file, and specify a name for the file (or accept the default name, SCHEMA_<number>.DMP). Click the Download File button.

To upload a schema:

1. Ensure that an empty schema, and a tablespace for it, are created on the database server. (See the *Governance, Risk and Compliance Installation Guide*.)
2. In fields next to the Upload button, enter the username and password for the empty schema. Click the Upload button.
3. An Import File dialog opens. Navigate to, and select the file you want to import, and click the Upload File button

Worklist Values

Fields available in the page opened from the Worklist tab apply only if GRC is installed with Service Oriented Architecture (SOA). Typically, these fields are set during installation and would not be changed subsequently. See the *Governance, Risk and Compliance Installation Guide* for information on setting these fields.

Setting Security Values

The Security tab opens a page in which you can set login, password, and other security values.

Click on the Security tab and enter values for any combination of the following properties:

- **Maximum Login Attempts:** Enter the number of times a user may enter an incorrect user name or password during login before being locked out of GRC.

(Administrators can use the Manage Users page to unlock user accounts. See page 3-7.)

- **Elapsed Days Before Password Expires:** Enter the number of days for which GRC login passwords remain valid. When each user's password expires, the user is prompted to create a new one during login.
- **Use Basic Authentication for Web Service:** Select the checkbox as one step in integrating GRC with an application whose database shares its user information through LDAP technology. (See "User Integration" on page 5-4).
- **Schedule Security Optimization:** Create or modify a schedule on which worklists are regenerated. Click on the Schedule Security Optimization button. A Schedule Parameter dialog opens. Enter values that set the name of the schedule, its start date and time, the regularity with which worklists should be refreshed, and an end date (if any). Then click on the Schedule button.

(A worklist is a record of, and link to, a task that a user must complete; each user has his own set. Changes to GRC security components may alter the rights of individual users, making them ineligible to open worklists to which they previously had access. When such changes are made, worklist regeneration ensures that users see only the worklists they should.)

When you finish setting values, click on Actions > Save.

Analytics

GRC may incorporate Oracle Fusion GRC Intelligence (GRCI), which provides dashboards and reports that present summary and detailed views of EGRM or EGRCC data. If so, GRCI makes use of a "data analytics" (DA) schema, which is distinct from the principal GRC database schema. Moreover, GRCI makes use of Oracle Business Intelligence Enterprise Edition (OBIEE).

The Analytics tab of the Manage Application Configurations page records values that embed GRCI within a GRC instance: In the Data Analytics Configuration section, an administrator enters values that establish a connection to the DA schema. In the GRC Intelligence Configuration section, an administrator enters values that set up OBIEE for use with GRC. In the Intelligence Page Configuration section, an administrator selects, and optionally renames, the GRCI dashboards that are to appear in the GRC instance.

Typically the fields in all these sections are completed during GRC installation (and their completion is dependent on other procedures being performed). Typically they are not changed subsequently. See the *Governance, Risk and Compliance Installation Guide*.

However, during installation or at any time afterward, you can create or modify a schedule on which the DA schema is refreshed. Click on the Schedule Data Analytics Update button (in the Data Analytics Configuration section). 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. Finally, click on Actions > Save.

User Integration

GRC can be integrated with an OID LDAP server that manages GRC users. Fields available in the page opened from the User Integration tab record values required for GRC to connect to the LDAP server. Typically, these fields are completed during GRC installation and are not changed subsequently. For more information, see the *Governance, Risk and Compliance Installation Guide*. (Also, see the discussion of the Use Basic Authentication for Web Service field on page 5-3.)

Configuring Notifications

You can set up GRC to alert users when tasks within GRC require their attention — when worklists are generated in EGRCCM or EGRCC.

EGRCC can alert result investigators not only when incidents await their review, but also when AACG preventive analysis requires approval of a role assignment to a business-application user. In the latter case, you can also configure EGRCC to inform that user of the approval decision.

GRC uses your email system to alert users to pending worklists. To establish a connection with your SMTP server and set a schedule on which email messages are sent, click the Notification tab and enter the following values:

- Notification Server
 - User Name: The user name with which one would log on to the SMTP server. This value is required only if access to the SMTP server requires authentication.
 - Password: The password with which one would log on to the SMTP server. This value is required only if access to the SMTP server requires authentication.
 - Confirm Password: The SMTP server password entered in the Password field. This value is required only if access to the SMTP server requires authentication.
 - Port Number: The port number at which the SMTP server communicates with other applications.
 - Server Name: The host name for the SMTP server your company uses for sending email.
 - Sender Email Address: An address that appears in the “From” line of email messages generated by the Notification function.
 - Application URL: The URL for your instance of GRC. This takes the form `http://host:port/grc`, in which *host* is the fully qualified domain name of your GRC server, and *port* is the port number selected for it when its web application server was configured during installation.
 - Enable SSL Authentication: Select this check box if access to your SMTP server requires authentication; clear the check box if it does not. If authentication is required, the User Name, Password, and Confirm Password fields must also be populated (see above).

- Enable Notification: Select this check box to activate the sending of worklist alerts to GRC users, or clear it to inactivate sending them.
- Notification Schedule
 - Start Date: Enter a date (in the format *mm/dd/yyyy*) on which the sending of email alerts should begin. Alternatively, click on the icon to right of 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.
 - Start Time: Enter a time (in the format *hh:mm*) at which the sending of email alerts should begin on your start date.
 - Hourly Interval: Enter a number that expresses the period (in hours) between which email alerts are sent.
 - Run Now button: Click to send email alerts once, immediately. To use this option, you need not enter values in the scheduling fields. If, however, a schedule has been set, it will continue to be honored; the use of the Run Now button does not affect it.
- Notification Content
 - Include All Worklist Entries: Select the check box to cause email content to include a list of worklist items appropriate for the recipient.
 - Generate User Provisioning Notification: Select the check box to activate the feature that informs business-application users about approval decisions concerning their roles. (This field appears only if you run EGRCC.)

When you finish entering values, select Actions > Save. In response to a prompt, restart the server.

Purging Incidents

Ordinarily, records of EGRCC incidents remain in the Incident Management page even after they have reached an end status (Resolved, Control Inactive, or Closed). The potential exists, therefore, for the number of incidents available for viewing to become large and unwieldy. To remedy this, you can use a Maintenance tab in the Manage Application Configurations page to purge incidents (at all statuses) generated before a date that you specify. The Maintenance tab applies only to EGRCC (the CCM module), not to EGRCCM (the Financial Governance and custom modules).

Note the following:

- When an incident is purged, all change history associated with the incident is also purged.
- Although an incident may be purged in GRC, the risk it represents may continue to exist in a business-management application: a user may still have access to conflicting access points, or a risky transaction may remain unresolved. If so, the next run of continuous controls will regenerate the incident in GRC. However, any status or comments assigned to the incident before it was purged are lost.
- A simulation feature enables users to forecast the effect of AACG incident cleanup in business-management applications. If you purge a set of AACG

incidents upon which a simulation had been based, you must rerun the simulation to update its results.

- If other jobs, such as control analysis or data synchronization, are running, a purge job will run only after those jobs are completed. If one GRC user runs a purge job while another is viewing an incident included in the purge, that incident is purged only after that second user navigates away from it.
- Reports generated before a purge will continue to show records of purged incidents, even though those incidents no longer exist in GRC.

To purge incidents:

1. Click on the Maintenance tab.
2. In a Control Type field, select the value *Access* to purge AACG incidents, *Transaction* to purge ETCG incidents, or *Both* to purge both types of incident.
3. In a Datasources field, select one or more datasources for which you want to purge incidents. To select one datasource, click on it. To select a continuous set, click on the first, hold down the Shift key, and click on the last. To select a discontinuous set, hold down the Ctrl key as you click on datasources.
4. In the Created On or Before Date field, select a date; GRC purges incidents generated on or before that date. 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.
5. Click on the Run button.
6. A confirmation message appears. Click on its OK button.

Application Datasources and Libraries

Use the Manage Application Datasources page to set up Oracle EBS, PeopleSoft, Oracle Fusion, and other datasources for use with EGRCC, and to synchronize data for those datasources. To open the Manage Application Datasources page, select Setup and Administration under Tools in the Navigator, then Manage Application Datasources under Setup.

Use a Manage Application Libraries page to upload business objects or patterns, both for use in EGRCC models and controls, or connectors to link GRC to datasources other than Oracle EBS or PeopleSoft (for which GRC uses a default connector). To open the Manage Application Libraries page, select Setup and Administration under Tools in the Navigator, then Manage Application Libraries under Setup.

Both of these pages apply to EGRCC. If you use EGRCC exclusively, information in this chapter does not apply to you.

Configuring Datasources

To set up an Oracle EBS or PeopleSoft datasource, you need only supply values for fields on the Manage Application Datasources page.

For Fusion, you must first install a connector and perform other configuration procedures (see the *Governance, Risk and Compliance Installation Guide*). Moreover, the values you enter for a Fusion datasource differ from those you would enter for an Oracle EBS or PeopleSoft datasource. The Fusion values reflect an interaction between GRC, Oracle Identity Management, and Oracle Internet Directory (OID), an LDAP repository whose identity store is managed by Oracle Identity Management.

To configure a new datasource:

1. In the Manage Application Datasources page, click on Actions > Create New. A Create Datasource pop-up window opens.
2. Enter the following values:
 - Datasource Name: Create a name for the datasource. (This name appears in a Manage Datasource window, in which users select datasources as they

create access or transaction models. It also appears in an Access Point List window, in which users select access points for inclusion in entitlements.)

- Description: Type a brief description of the datasource (optional).
- Application Type: Select the type of business application to which you are connecting — EBS, PeopleSoft, or Fusion.
- 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 transaction models. Only one datasource can have this value selected.

- Connector Type: For an Oracle EBS or PeopleSoft datasource, select Default. For Fusion, select the Fusion connector you installed prior to working in this Manage Application Datasources page; the correct value is *FusionConnector*.

For any other application, you would need to have created and uploaded a custom connector (see page 6-5); 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, MS SQL Server, or DB2 — 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. For Fusion, supply the FQDN of the LDAP provider (your OID instance).
 - Password: For Oracle EBS or PeopleSoft, enter the password for the business-application database. For Fusion, enter the password for the OID administrative user.
 - Port: For Oracle EBS or PeopleSoft, enter the port number that the business-application database uses to communicate with other applications. For Fusion, enter the port number for the OID instance identified in the Hostname field.
 - Service Name: For Oracle EBS or PeopleSoft, supply the SID value configured for the business-application database in the tnsnames.ora file. For Fusion, enter *Fusion*.
 - 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.) For Fusion, supply the username for the OID administrative user, preceded by *cn=*.

3. After entering values, click on the Test Connection button. 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.

Synchronizing Data

Periodically, you need to synchronize data used by EGRCC models and controls — capture changes made in the business application (datasource) in which the models and controls evaluate risk:

1. In the Manage Application Datasources page, select the row for the datasource with which you want to synchronize data.
2. Do any of the following:
 - Click on Actions > Synchronize Access. Alternatively, click on the Synchronize button in the tool bar, then on a Run Now option, and then on an Access option. This causes data used by AACG to be synchronized once, immediately.
 - Click on Actions > Synchronize Transaction. Alternatively, click on the Synchronize button in the tool bar, then on a Run Now option, and then on a Transaction option. This causes data used by ETCG to be synchronized once, immediately.
 - Click on Actions > Schedule Synchronize. Alternatively, click on the Synchronize button in the tool bar, then on a Schedule option. A Schedule Parameter dialog opens, in which you may create a schedule on which any number of synchronization operations run automatically. Select the Access or Transaction check box to synchronize data used by AACG or ETCG (or select both), and enter values that set the name of the schedule, its start date and time, the regularity with which the synchronization should occur, and an end date (if any). Then click on the Schedule button.

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.

Uploading Business Objects

As you create EGRCC models and controls, you work with business objects, each essentially a business-language label for one or more database tables that hold information pertinent to access or transactions. Business objects contain attributes, each a business-language name for a column within the selected object. Although GRC comes with a selection of business objects already configured, more will be developed over time. As they are made available, you can upload them from files to your GRC implementation.

For each business object, upload two files (both of which are in .OWL format):

- **Business Object Dictionary:** This is the Semantic Data Dictionary (SDD). It is a collection of generic business definitions of a single object regardless of any application instance.
- **Business Object Mapping:** This is the Semantic Data Mapping (SDM). This is the mapping of the attributes of the associated Business Object Dictionary to the physical store specific to an application (Oracle E-Business Suite or

PeopleSoft). Examples of attributes for a Business Object called Customer include Customer Name, Address Line 1, Zip, and Customer ID.

To import business objects:

1. In the Manage Application Libraries page, click on the Business Objects tab.
2. To import a business object dictionary file, click on Actions > Import Business Object Dictionary. To import a business object mapping, click on Actions > Import Business Object Mapping. To import a business object, you must do both (although, of course, as distinct operations). You cannot import a mapping file until you have imported the related dictionary file.
3. In either case, an Import File pop-up window opens. Click on its Browse button.
4. A file-upload dialog opens. In it, navigate to and select the .OWL file you want to import. The path and name of the file then populate the field next to the Browse button in the Import File window.
5. With the file selected, click on the OK button. A pop-up message reports the status of the import operation. Click on its OK button to clear it, and then click on the Close button in the Import File window.

When the dictionary file is imported, a new row in the Business Objects grid displays information about it; among other values, a Type field displays *Dictionary* and a State field displays *Formatted*. When the related mapping file is imported, the row is updated; the Type field continues to display *Dictionary*, but the State field changes to display *Mapped*.

You can also export business object mappings to files:

1. Select a mapping in the Business Objects grid.
2. Select Actions > Export Mapping Template.
3. Follow prompts to save the export file to a location of your choice.

Uploading Patterns

“Patterns” are statistical functions, supplied by Oracle, that may be used in transaction models and controls. Independently of GRC releases, Oracle may issue files (in .jar format) that contain patterns. To upload these files:

1. In the Manage Application Libraries page, click on the Patterns tab.
2. Click on Actions > Import.
3. An Import File pop-up window opens. Click on its Browse button.
4. A file-upload opens. In it, navigate to and select the file you want to upload. The path and name of the file then populate the field next to the Browse button in the Import File window.
5. 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.

In the Patterns page, rows display information about patterns you’ve uploaded — for each, the name, description, and version.

Uploading Connectors

A custom connector uses ETL technology to collect data from a business-management application and provide it in a format that GRC recognizes. A default connector, provided with GRC, does this for instances of Oracle EBS and PeopleSoft. Custom connectors may be developed (outside of GRC) to do the same for other business-management applications, and then uploaded to GRC. Once uploaded, a custom connector would be selected for a particular datasource in the Manage Application Datasources page (see page 6-1).

1. In the Manage Application Libraries page, click on the Connectors tab.
2. Click on Actions > Import.
3. An Import File pop-up window opens. Click on its Browse button.
4. A file-upload opens. In it, navigate to and select the file you want to upload. The path and name of the file then populate the field next to the Browse button in the Import File window.
5. 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.

In the Connectors page, rows display information about the connectors you've uploaded — for each, the name, description, and version.

To delete a connector, select its row, and then select Actions > Delete. Respond to a message that prompts you to confirm the deletion.

Other Setup Options

Use certain setup pages to manage lookup tables, manage content types, manage installation options, manage URL repositories, and manage assessment results. Among these tasks, managing lookup tables and managing content types apply both to EGRCC and EGRCM; the others apply to EGRCM only.

To open any of these pages, select Setup and Administration under Tools in the Navigator, then select the applicable option in the Setup list of tasks.

Managing Lookup Tables

As you create or edit GRC components, you are often able to select among entries in lists of values — for example, perspective types, assessment types, or reason codes for closing issues. In each case, the entries you can select are stored as “lookups.”

Each LOV has its own set of lookups, and a “lookup type” distinguishes lookups belonging to one LOV from those belonging to others. Within a given lookup type, each entry correlates a “lookup code” to a “meaning,” the latter being the text that actually appears in an LOV. Each entry may also have a description.

You can update the meanings and descriptions of delivered lookups, and you can add new values to some delivered lookup types. You can also create new lookup types to support user-defined attributes.

To create a lookup, first determine its lookup type: Identify one value in the LOV in which the lookup is to appear. For example, if you are creating a new perspective type, look at the Type field in the Create Perspective Hierarchy page and note one of its values, such as Major Process. Then, in the Manage Lookups page, enter that value in the Meaning field of the Search panel, and click the search button. The Search Results panel then presents one row that displays the lookup type to which you want to add — in this example, `GRCM_PERSPECTIVE_TYPE`.

Then, in the Manage Lookups page:

1. Select Actions > Create Lookup. A Create Lookup page opens.
2. In the Lookup Type field, enter the lookup-type value you’ve just identified.
3. Enter a code in the Lookup Code field. In the Meaning field, enter text that will actually be presented in an LOV.

4. Optionally, describe the lookup in the Description field.
5. Select the Used for User Defined Attribute check box only if you are creating a lookup to support a user-defined attribute.
6. Click the Save button.

To edit a lookup:

1. In the Manage Lookups page, search for the lookup you want to edit: In the Search panel, enter any combination of type, meaning, and description values, and click the Search button.
2. In the Search Results panel, click on the row for the lookup you want to edit, then select Actions > Edit Lookup.
3. An Edit Lookup field opens. Modify the meaning or description value, or select (or clear) the Used for User Attribute check box. (The lookup type and lookup code are presented as read-only values; you cannot edit them.)
4. Click the Save button.

Managing Content Types

You can attach files to GRC objects that support attachments, typically to provide additional documentation of them. For each attachment, you must select a content type. The Manage Content Types page enables you to create, edit, or delete these types. Each consists of a content code and a description, the latter being the text you see as you are selecting a content type for an attachment.

To create a content type, select Actions > Create in the Manage Content Types page. A Create Content Type pop-up opens; in it, enter a content code and a description, and click the Save button. The new type is then listed in the Manage Contents Type page.

To edit a content type, click on its row in the Manage Content Types page, then select Actions > Edit. An Edit Content Type pop-up opens; in it, modify the description value for the type you've selected. (The pop-up displays the content code as a read-only value; you cannot modify it.) Then click on the Save button.

You can delete a content type only if it has not been selected as the type for any attachment. To do so, click on its row in the Manage Content Types page, then select Actions > Delete.

Managing Installation Options

The Installation Options page enables you to specify the currency used by your installation of EGRCM. (Only one currency is supported throughout the installation.) In the Currency list box, select the currency you want to use, then click the Save button.

Managing Assessment Results

You can edit the responses from which users may select as they perform assessments. In the Manage Assessment Result page, locate the response you want to edit, and modify its Response Name value. Then click the Save button. You cannot modify response codes. You cannot add new responses or delete existing responses.

Managing URL Repositories

Use the URL repository to manage links that are available when you create user-defined attributes with the link data type.

To add a URL to the repository, select Actions > Create in the Manage URL Repositories page. A Create URL Repository page opens; in it, enter a name, a description, and a URL address. Then click the Save button. The new type is then listed in the Manage URL Repositories page.

To edit an entry in the URL repository, click on its row in the Manage URL Repositories page, then select Actions > Edit. An Edit URL Repository page opens; in it, modify any of the name, description, or URL address values. Then click the Save button.

You can delete a repository entry only if it is not associated with any UDA. To do so, click on its row in the Manage URL Repositories page, then select Actions > Delete.

Module Management

For EGRCM, you can configure the default Financial Governance module, and you can use a standard template to create new modules. You can also create user-defined attributes (UDAs) — information added to a given object within a module, to extend its definition.

EGRCC runs as a Continuous Control Monitoring (CCM) module, but you cannot create other EGRCC modules.

So, most module-management functionality applies to only to EGRCM. One exception is Manage Module Perspectives (page 8-4). In both EGRCM and EGRCC, a perspective hierarchy is unavailable for use until it is associated with object types. Manage Module Perspectives enables you to configure these associations. A second exception is Data Migration (page 8-4), which you can use to import all types of operational data into EGRCM, and perspectives into EGRCC.

Managing Modules

To create a module, select Manage Modules in the Module Management tasks under Setup and Administration; then select Actions > Create Module. A Create Module page opens.

1. Name the module and select the standard template.
2. In the Select Module's Objects area, click on the check box for each of the base, risk, and control objects you want to include in the module.
3. A square representing each object appears in the Select Object Relationships area of the page. In each object, select check boxes to establish relationships with other objects. (For example, you select Base Object A and Risk Object A. The square representing Base Object A contains a check box labeled Risk Object A. Click it to indicate that Risk Object A is related to Base Object A.) Or clear check boxes to sever relationships.
4. Relabel the objects you've selected. This is optional, but recommended, so that objects have names that are meaningful to you. Click the Relabel button and, a Relabel Objects pop-up appears. In it, type a new name for each object in its Relabeled Value field, then click the OK button.
5. Save your work.

Configuring Module Objects

You can choose which features are available for each object within an EGRCM module, and define how assessments are conducted for the object.

First, select the object you want to configure: Select the Configure Module Objects entry under Module Management in the Setup and Administration tasks. A Manage Configuration Options page opens, displaying a list of modules. Click on the icon next to a module name to reveal a list of its objects. Click on an object name, and then on Actions > Edit. An Edit Configure Options page opens.

In a Configurable Options section of the page, you can hide or display features, according to your business requirements.

- **Result:** Determines whether a Result tab appears in the Manage page for an object. Select Show (the default) or Hide. If the tab appears, the object can display “incidents” generated in the CCM module, and assigned in that module to objects in other modules. This option applies to processes, other base objects, risks, and controls.
- **Consequence:** Determines whether consequences are displayed with related events in the Events region of the Create, Edit, and Manage Risk pages. Select Hide (the default) or Show. This option applies only to risks.
- **Event:** Determines whether the Event region is available for use in the Create, Edit, and Manage Risk pages. Select Hide (the default) or Show. If events are hidden, consequences are also hidden. This option applies only to risks.
- **Treatment:** Determines which treatment options are available in the Manage Risk page. The default setting is Hide and Default: treatments and treatment plans are hidden, but related control stratification is exposed. You may instead select Hide: treatment, treatment plan, and control stratification are hidden and, for the Financial Governance module, risk does not have a relationship to control within Risk Management. A third possible selection is Show: treatment, treatment plan, and control stratification are available. This option applies only to risks.

In an Assessment Activity Definitions section, you can determine the assessment activities that are available for the object. Under Assessment Activity Definitions, select an Include check box for each activity you want. Then click on each of the included activities to select the following values for each activity:

- **Guidance Text:** Edit a broad statement of purpose a user may consult while completing the assessment activity. Or, restore a default statement.
- **Activity Question:** Create or edit the question a user is required to answer while performing an assessment.

For the activity you select, you can also view Response Details. This section lists responses users can make while completing assessments. Each response consists of a code (“Response”) and a plain-language statement (“Response Name”). Response Names can be edited in the Manage Assessment Results page (see page 7-3). The codes cannot be edited, and the selection of responses for a given activity type cannot be changed.

Managing User-Defined Attributes

You can add attributes to objects such as risks, controls, base objects, perspectives, issues, assessments, and survey templates. These attributes appear automatically in the Additional Details region of the object Create, Edit, and Manage pages. When creating a user-defined attribute (UDA), you can select properties, such as data type.

First, select the object to which you want to add UDAs: Select the Manage User Defined Attributes entry under Module Management in the Setup and Administration tasks. A Manage User Defined Attributes for Object Types page opens, displaying a list of modules. Click on the icon next to a module name to reveal a list of its objects. Click on an object name, and then on Actions > Edit. A new Manage page opens for that object. In it, select Actions > Create, or click on an existing UDA and select Actions > Edit.

Depending on the data type you select for your UDA, you might have to specify:

- Display label: Enter a label displayed in the UI and in reports.
- Name: Specify a name for the UDA. This is free-form text.
- Description: Enter a detailed description of how the UDA will be used.
- Data type:
 - Number.
 - Date.
 - String Translatable: A character string that supports translation.
 - String NonTranslatable: A character string that is not translated in codes. This is the only type that supports LOVs or value sets.
 - Link: Can be used to specify a standard URL.
- Control type: The available control types depend on the data type you have selected. They can include text box, check box, dropdown, date picker, multiple line text box. If you have chosen the Link data type, you will not see the control type option.
- Lookup Type: For the String NonTranslatable data type, you can specify an existing value set from which users can select a value.
- URL: If you have specified the Link data type, select a URL. The URLs you can choose from are stored in the URL Repository. The link appears within the UDA Additional Details section as an active hyperlink.
- Order: Specify the order in which this UDA should appear in the Additional Details region for the object.
- Assessment types: Specify the assessment types on which the UDA will be used, for all objects that support assessment. (The UDA appears with the types of assessment you select, and not on the object being assessed.)
- Status: Choose Active or Inactive.
- Required: Choose this option if you want the UDA to be required. This means that users will not be able to save the object unless this field contains valid data.

Managing Module Perspectives

Although perspective hierarchies are created in Perspective Management (see chapter 2), each hierarchy becomes available for use with objects only after being associated with that type of object in a module. For the CCM module, you can create associations to model, continuous control, or incident. For Financial Governance and other EGRCM modules, you can create associations to risk, control, or base object (Process in the Financial Governance module).

To associate a perspective with an object:

1. In Manage Module Perspectives, click on the module for which you want to associate perspectives with objects, and then select Actions > Edit.
2. A page opens for the module you've selected. In it, choose Actions > Create.
3. An Add Perspective pop-up window opens. In it, enter the following values:
 - Name: Choose the name of the perspective.
 - Associated Object: Select the object you want to associate with the perspective.
 - Required: Specify whether at least one perspective value must be selected for each object of the associated type. For example, you might require that a user select an Organization perspective value when he creates a new process object for the Financial Governance module.
 - Status: Specify if this association is active or inactive. You can modify this setting later.
4. Save your changes, then click the Done button.

You can also click on the row for a configured association between a perspective and an object, and select Actions > Edit to modify its status or whether the perspective is required for the object. (Before data exists in the module in which you are working, you can set the Required check box as you wish. After data exists in the module, however, a required perspective may be changed to optional, but an optional perspective cannot be changed to required.) Or, select Action > Delete to delete the association.

Data Migration

A Data Migration utility enables you to upload operational data for the Financial Governance module or any new EGRCM module, or perspective data for the CCM module. The procedure involves generating an XML template that reflects the specific configuration of the module, updating the template with your operational data, and running an import process.

Operational data includes object specifications, how objects are associated to one another, transactions against the objects (such as issues, remediation plans for issues, action items for base objects, risk analysis and evaluation, and assessments), and attachments.

The Data Migration utility supports both initial and incremental loading of operational data:

- **Initial Load:** The import file contains operational data that is new to the module and has no association to data already existing in the module. (Initial Load can be run even when other data already exists in the module.)
- **Incremental Load:** The import file once again contains operational data that is new to the module, but it may define associations to data that already exists in the module, or new values for perspectives that already exist in the module. New transaction data for existing objects can also be imported during an incremental load, but the update of existing transactions is not supported.

Refer to the *Oracle Enterprise Governance, Risk and Compliance Implementation Guide* for complete details of how to import data. In general, data migration includes the following tasks:

- Create the module for which you intend to upload data, if it does not exist already. Use the application to configure objects, perspectives, UDAs, or other operational data within that module.
- In the Data Migration page, click in a row representing the module into which you want to upload data, and then click the Create Import Template button to create a template. A Create Import Template dialog offers the option to create a template with or without data. If you choose the with-data option, the template contains any operational data already configured for the module. (The export of this data is completed in the GRC Manage Jobs page; see page 9-qq.)
- Edit the template to update existing data, add records for new data, or both. The template is an Excel workbook in which each sheet contains data defining individual instances of an object, association, transaction, or attachment.
- Save the template as an import file. It must be saved as an XML spreadsheet (.xml). In the Data Migration page, click the Import Data File button to import the data.

Jobs and Scheduling

“Jobs” are individual requests to synchronize data, evaluate models or continuous controls, export results, generate reports, or perform other background tasks. Some jobs can be run on demand, or can be scheduled to run. In general, a job is run or scheduled from a page to which it applies — for example, one might synchronize data from the Manage Application Data page or run controls from the Continuous Control Management > Manage Controls page.

In the Manage Jobs page, users may view jobs, manage exported and imported data, cancel jobs, or purge job history. In the GRC Navigator, select Tools > Setup and Administration > Administration > Manage Jobs to open this page.

Managing Jobs

Each row in the Manage Jobs page presents the following information about one occasion when a job was run. Values include:

- **Job ID:** An identification number assigned internally to the job by GRC.
- **Name:** The name of the job that was run.
- **Start Date and End Date:** The dates and times on which the job began to run and finished running.
- **Status:** The current state of a job. Most statuses are assigned by GRC. These include Not Started, Started, Queued, Pause Requested, Paused, Completed, and Error. GRC updates the status until a final state (either Completed or Error) is reached.

GRC prioritizes jobs. The Pause (or Pause Requested) status indicates that GRC has suspended (or is attempting to suspend) a job in order to undertake a higher-priority job. Only GRC can pause jobs or request that they be paused; there is no way for a user to do so.

Users may, however, cancel jobs. When a user does, the job status changes to Cancel Requested or, ultimately, to Canceled.

- **Message:** An informational message about the job status. When the job has finished running, the Message field displays a “Job completed” link; click on it to open a Job Detail window, which displays information about the job. The Job Detail window may also contain a link to the download file created by an export

job (or to a display of status for an import job). To close the Job Detail window, click on its OK button.

- Run By: The user name of the user who ran the job.

Managing Import and Export Jobs

From the CCM module, users can export or import models, global conditions, or continuous controls. Users can also export templates containing perspective data (from CCM) or perspective and other operational data (from Financial Governance or other EGRCM modules); a template then serves as a vehicle for the import of new perspective or operational data. Although an export is initiated within the module that contains the export data, it is completed from the Manage Jobs page.

1. Initiate an export from the page for managing CCM models, global conditions, or controls, or from the Data Migration page among the GRC tools. A message presents a job number; note the number, then click on the OK button to close the message. (See “Data Migration” on page 8-4. Or, for information about initiating model, global condition, or control exports, see the user guides for AACG and ETCG.)
2. In the Manage Jobs page, locate the row displaying the job ID you noted in step 1. In its Message cell, click on the Job Completed link.
3. The Job Detail window opens. In it, click on the Job Results link.
4. A File Download window offers you options to open or save the export file. Click on its Save button and, in a Save As dialog, navigate to a folder in which you want to save the file. The file is saved in .xml format.
5. Close the Job Detail window (click on its OK button).

When a data file is imported, its Job Detail window (opened once again from the Job Completed link in its row on the Manage Jobs page) also contains a Job Results link. It opens a page displaying status and details of the import.

Canceling a Job

If you have update permission to the Manage Jobs page, you can cancel a job whose status indicates that it is still in progress. Click on the Row identifying the job, click on the Cancel Job button, and respond to a message asking you to confirm the cancellation. In this case, the status changes to Cancel Requested or, ultimately, to Canceled.

Purging Job History

If you have update permission to the Manage Jobs page, you can use a Purge feature to remove entries from the page:

1. Click on the Purge button in the tool bar. A Purge Job History dialog appears.
2. In the “days old” field, enter a number of days before the present date. This effectively defines a purge date; jobs completed after that date are kept, and those completed before that date are deleted. For example, if the current date is

July 30 and you enter the value 1, your purge date is July 29 and only those jobs completed on July 30 will be retained.

3. Click on the Purge button. A message confirms the purge operation; click its OK button to clear it.

Managing Schedules

A job may be scheduled to run, and typically the schedule is created in the page to which the job applies; the job may be run manually from that page as well. For example, one may update a data analytics schema, or schedule it to be updated, from the Manage Application Configurations page. However, any schedule created elsewhere is listed in the Manage Scheduling page, where you may modify schedules or run jobs manually.

To open this page, select Tools > Setup and Administration > Administration > Manage Scheduling.

Viewing Schedules

In the Manage Scheduling page, each row presents information about a job scheduled to run in the future.

Values include:

- **Schedule Name:** The name assigned to the schedule when it was configured.
- **Name:** The name of the job itself — for example, the name of a report if the scheduled job is to generate the report.
- **Last Run Date:** The date and time on which this schedule last caused the job to be run.
- **Next Run Date:** The date and time on which this schedule will next cause the job to be run.
- **Scheduled By:** The user name of the EGRCC user who created the schedule.

Modifying Schedules

If you have update permission to the Manage Scheduling page, you can modify or discontinue a schedule:

1. Click on the row for a schedule, then click the Edit button. A Schedule Parameter dialog opens. Each schedule is specific to the type of job being scheduled, and each dialog is specific to the schedule it is designed to set.
2. Do either of the following:
 - Enter new values in fields, and make new selections among radio buttons, to define a new schedule, and click on the Reschedule button. Then new schedule is then in force.
 - Click on the Unschedule button. All values are then removed from the Schedule Parameter dialog, and the job is no longer scheduled to be run.

Running Jobs Manually

From the Manage Scheduling page, you can run any job for which a schedule has been created. Doing so runs the job immediately, and does not affect the schedule — the job will run again when its schedule next determines that it should. To run a job manually, click in the row representing its schedule, and click the Run Now button. An Information pop-up window reports that the job is queued; click its OK button to close it.