Oracle® Enterprise Governance, Risk and Compliance

User Guide

Release 8.6.4.7000

Part No. E40661-01

May 2013

ORACLE®

Contents

4 Reporting

5 Application Configuration Management

6 Application Datasources and Libraries

7 Other Setup Options

8 Module Management

9 Jobs and Scheduling

A Appendix: Seeded Lookups

Preface

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

An Oracle Enterprise Governance, Risk and Compliance (GRC) platform hosts several products — Oracle Application Access Controls Governor (AACG), Oracle Enterprise Transaction Controls Governor (ETCG), and Oracle Enterprise Governance, Risk and Compliance Manager (EGRCM).

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 AACG and ETCG run. (Moreover, GRC "Tools" offer functionality used across GRC modules.)

This *Enterprise Governance, Risk and Compliance User Guide* covers functionality common to GRC applications (although the *Governance, Risk and Compliance Installation Guide* covers some setup and administration topics).

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

1

Introduction

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

- Oracle Application Access Controls Governor (AACG) and Oracle Enterprise Transaction Controls Governor (ETCG) enable users to create models and "continuous controls," and to run them within business applications to uncover and resolve segregation of duties violations and transaction risk. These applications are two in a set known collectively as "Oracle Advanced Controls."

- 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. In 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 GRC.

These GRC components run as modules in a shared platform. AACG and ETCG run 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 AACG, ETCG, 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 AACG and ETCG. Others, such as creating "content types" or managing "URL repositories," are specific to EGRCM. Nevertheless, these component-specific setup tasks are discussed in this *User Guide*.)

- Module management. Most module-management features apply only 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 AACG, ETCG, and EGRCM.

- Jobs and scheduling. Users can schedule and manage background tasks such as updating a "data analytics schema," evaluating continuous controls, exporting results, or generating reports.

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.

- 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 the CCM module, the following are suggested maximum amounts:

- AACG entitlements per control: Two.

- AACG access points per entitlement: Fifteen.

- ETCG model logic: Maximum combination of three business objects and one pattern filter.

- ETCG business objects per control: Five.

- AAGC global path conditions per datasource: Thirty.

- 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 3-6), or updated by him in his user profile (see page 1-6).

GRC 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.

• Generally, GRC 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, GRC 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 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 Financial Governance list offers links to pages in which you can manage objects within this module — risks, controls, processes, and issues. For each new module you create, a comparable list appears in the Navigator.

The list for the Continuous Control Monitoring module includes two links: Continuous Control Management enables you to create models, continuous controls, and their components; run them; and review model results. From Result Management, you can resolve the incidents generated by controls.

A Tools list provides access to features that apply across modules, such as perspective management, assessment management, or administrative features.

Once you make a selection in any of these lists, GRC opens an overview page for the item you've selected, and displays a Tasks list with links to pages offering functionality appropriate for that item.

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 and Overview Pages

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.

  In the CCM module, a worklist is a record of incidents generated by a control for which you are a result investigator.

  In the Financial Governance module (or any custom module), the worklist displays a name for the task, a description, and the name of the object to which the task applies. The task description is a brief statement of the action you are intended to take. "Draft" indicates work that you have begun but not yet completed, such as a control that you have saved but not yet submitted for review. Other task descriptions, such as "Review" or "Complete Assessment," are self-explanatory.

  To view your worklists, select the Worklists tab in the Pending Activities area of your home page.

- For CCM purposes, a notification is a record of a continuous control that you created. In Financial Governance and other modules, a notification is a record of a task in which you have an interest. In either case, no action is required of 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.

- 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.

For Financial Governance (or any custom module), an overview page opens when you select any object in the Navigator. This page displays your worklists and notifications for that object.

In the CCM module, notifications also appear in a control-overview page that opens when you select Continuous Control Management in the Navigator. Worklists also appear in a result-overview page that opens when you select Result Management in the Navigator.

You can search among worklist and notification entries. See "Searching Among Records" (below).

If your GRC instance includes Oracle Fusion GRC Intelligence (GRCI), and if your roles give you access to GRCI, your home page or object-overview pages may also include an Intelligence tab. Click on it to view GRCI dashboards and reports.

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

Searching Among Records

GRC management and overview pages display lists of items. On each page, GRC implements a "seeded search" to display the most expansive possible list of items appropriate for the user who is currently logged on — for your purposes, you. On each page, you can use search features to create customized lists of items.

In each of these pages, use a Search panel to specify search parameters. (In each page, first expand the Search panel by clicking on its > button.) You can create a basic or advanced search. You can also save searches so that you can use them repeatedly.

Basic and Advanced Searching

By default, each Search panel is set to perform a basic search. You can click an Advanced button to set up an advanced search; from the advanced panel you can click a Basic button to return to the basic search.

A basic search presents a set of fields in which you can enter values for commonly used search parameters. (All search parameters correspond to selections you make as you create or otherwise work with the object for which you are searching.) In the Manage Controls page, for example, you can set values for status, control name, priority, type, and datasource.

For a basic search, text-entry fields assume a "Starts With" operator (the search finds records in which the specified value starts with the text you enter). Most LOVs assume an "Equals" operator (the search returns records in which the specified value matches the one you select), although an LOV that enables you to select "All" assumes an "In" operator (returning records in which the specified value is any of those you select).

An advanced search typically expands the number of search parameters you can use. It also enables you to select among a variety of operators for each parameter. You may add search parameters: Click on the Add Fields button. A list of fields appears; in it, click on the field you want. (An added field appears with a red × symbol. Click on that symbol to remove the field from the Search panel.)

To complete either type of search, enter values (and, for an advanced search, select operators) for any combination of available parameters. For text-entry fields, you can use the percent sign as a wild-card character. Also select a Match value: Click

the All radio button to require records to match all of the parameters you specify, or the Any radio button to permit records to match any one (or more) of the parameters you specify. Then click the Search button.

To clear search values and restore the original list of items, click the Reset button. (This actually implements criteria for a search currently selected in the Saved Search field.)

Saving a Search

You can save any basic or advanced search, then run it any number of times (or even make it the default for the page in which you are creating the search).

In the page that displays CCM incidents, you can modify the formatting of the grid that lists the incidents. For this page, saving a custom search also saves formatting modifications. (To open this page, select Result Management under Continuous Monitoring in the Navigator, select Manage Incident Results among the Result Management tasks, and select Incident Results in a View By list box on the Incidents page.)

Formatting changes can include column width (drag the border of a column to expand or contract it), column placement (drag a column heading where you want it to appear), and sort order (left click in the heading of a sortable column). You can also add or remove columns (right-click on the header row, select check boxes for the columns you want, and clear check boxes for the columns you don't want).

By default, the page displays a "seeded" search — pending incidents for which the user who is logged on is a result investigator. You cannot save formatting changes to that search. (However, you can make formatting changes to the seeded search, save it under a new name as a custom search, and make that new search the default. In this case, the formatting changes are saved.)

In other pages, you can make similar formatting modifications to grids. However, while you can save searches on those pages, you cannot save their formatting changes.

To save a search:

1. Enter values for search parameters and click the Search button.

2. Click the Save button.

3. A Create Saved Search pop-up window appears. In it:

   • Enter a name for the search.

   • Select or clear a Set as Default check box. Selecting this box causes the search to run whenever you open the page in which you are setting up the search.

   • Select a Run Automatically check box to cause the search to be evaluated immediately as it is selected in a Saved Search LOV. Or clear the check box; if so you would need to select the search, then click the Search button.

4. Click on the OK button.

To run a saved search, select it in a Saved Search list of values. (If the Run Automatically option is not enabled for the search you select, also click the Search button.)

From the Saved Search LOV, you can select a Personalize option. A Personalize Saved Searches pop-up window appears. In it, select one of the saved searches. Then, you can click the Delete button to delete the search. Or, reset the Set as Default and Run Automatically options (set initially as the search was saved). Or set a third option: select a Show in Search List check box to ensure the search is listed in the Saved Search LOV, or clear the check box to remove the search from the LOV. Click on Apply to implement your changes, and OK to close the pop-up window.

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.

2

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 AACG and ETCG, 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 AACG and ETCG, 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 must also 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 the Issues tab to see records of issues raised against the hierarchy.

- Click on any of the nodes in the hierarchy, and an Item Details panel displays general details of its configuration, and records of its 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.

Creating Perspective Hierarchies

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 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.

   d. If you select desktop file, click the Browse button to navigate to, and select, the file you want. Select a content type, compose a title, and optionally enter a description.

      If you select url, enter it in the File Name/URL field, compose a title, and optionally enter a description. (Content type does not apply in this case.)

   e. To create additional attachments, repeat steps b through d for each.

   f. 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 node in the hierarchy, and an Item Details panel displays tabs in which you can view general details of its configuration, 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, save the hierarchy if you intend to work on it further, or submit it when it is ready for use by others. 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.

Editing Perspective Hierarchies

To edit a hierarchy, open it in the Edit Perspective Hierarchy page. (See "Managing Perspective Hierarchies" on page 2-2.) It's similar to the Create Perspective Hierarchy page; in general you can modify perspective values 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.

3

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 — at a minimum, that which exists at one or more specified states and is subject to a specified action. If a primary data role is to grant access to Financial Governance or CCM data, it also specifies the module that the role is to support.

  If a primary data role supports assessment activities in EGRCM, it further selects data 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, it specifies 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" defines a more broadly focused set of data, to which a user can apply the functionality granted in a job duty role. It may specify primary data roles, or other composite data roles, to combine the access granted by those roles.

  There are specialized types of composite role: A "custom perspective data role" limits the access defined by its constituent roles to data associated with specified perspective values. A "module data role" limits the access defined by its constituent roles to data belonging to a specified custom module. (Such a role would be created only for a custom module. For Financial Governance or CCM roles, the module is specified in a primary data role.)

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

- A "job role" comprises a job duty role and a composite 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 Enterprise 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 two filters. One specifies 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 other specifies an action that may be performed on data at the selected state. If the role is to grant access to Financial Governance or CCM data, a third filter specifies the module that the role is to support.

  If the role supports EGRCM 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 CCM 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, roles for use with CCM may contain filters that select perspective values representing datasources and business objects to which the role grants access. 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.

  In most cases, a datasource is a business application subject to CCM models and controls, although a datasource called GRC represents the GRC instance itself. 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. (If a role's business-object filter selects the perspective value for either of two objects — User or Access Entitlement — the datasource filter must select the perspective value for the GRC datasource.)

  A role that supports work with incidents, access requests, or path conditions must include a datasource filter, but not a business object filter.

- A module data role contains one or more filters that select composite data roles and a filter that specifies a custom module. The role limits the access granted by the composite roles to data associated with the module. (Such a role is created only for custom modules. For Financial Governance or CCM, the module is specified in primary data roles.)

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. 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, or DataRole. 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. An Import from LDAP window opens, but displays no users.

4. In search fields along the top of the window, enter search parameters. You can search on any combination of username, first name, and last name, and you can use the percent symbol (%) as a wild card character. (If you want to retrieve all possible users, enter the percent symbol in the username search field.) Press the Enter key.

   The page then displays users whose identifying values match your search criteria. (Only active LDAP users who are not already created as GRC users are listed. If an LDAP user has the same username as an existing GRC user, you cannot import that LDAP user.)

5. Put a check mark (click) in the Select field for each user you want to import.

6. 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.

4

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 which of the EGRCM, AACG, and ETCG applications you use (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 User Provisioning Report displays records of role assignments in business-management applications that were suspended, prevented, or allowed by AACG preventive processing.

- 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 for use with AACG, 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 Worklist Items 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 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.

5

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.

Installation Configuration

Fields in the Installation Configuration section of the Properties page record database connection settings. Typically, fields in this section are completed during GRC installation and are not changed subsequently. (During installation, you use a page titled ConfigUI. Apart from the name, it's identical to the Properties tab of the Manage Application Configurations page.) For more information on values appropriate for these fields, see the *Enterprise Governance, Risk and Compliance Installation Guide*.

Performance Configuration

Fields in the Performance Configuration section record settings that may optimize GRC performance. Although these fields may be completed during GRC installation, some may be modified subsequently. They include the following:

- Optimize Distributed Operation: Select the check box to increase the speed at which GRC performs distributed operations such as data synchronization.

- Optimize Appliance-Based Operation: Select the check box to optimize performance if the GRC application and GRC schema reside on the same

machine. Do not select this check box if the GRC application and schema do not reside on the same machine. When you select this check box, an ORACLE_ HOME Path field appears. In it, enter the full, absolute path to your Oracle Home — the directory in which you have installed the Oracle database that houses the GRC schema.

- Enable Graph Synchronization Date Limit: Data synchronization enables GRC to recognize data changes in each business application subject to models and controls. The process works differently for AACG and ETCG.

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

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

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

    When you select the check box, a Transactions Created As Of field appears. In it, enter the cutoff date for the synchronization of ETCG Transaction business objects. When you click in the field, a pop-up calendar appears. Click left- or right-pointing arrows to select earlier or later months (and years), and then click on a date in a selected month.

- Externalize Report Engine: Select the check box to enable the reporting engine to run in its own java process, so that the generation of large reports does not affect the performance of other functionality. However, select the check box only if you have installed GRC on hardware identified as "certified" in the *Oracle Governance, Risk and Compliance Certifications Document*; clear the check box if you use hardware identified as "supported."

- Enable Parallel Processing: Select this check box to enable multiple models and controls to be processed simultaneously. However, this feature requires, at minimum, 16 GB of RAM; 24 GB is preferred.

    When you select the Enable Parallel Processing check box, two fields appear. In a Number of Cores Available for Processing field, enter the number of processor cores you wish to devote to parallel processing; one core is devoted to each model or control selected for analysis, until as many cores as you select are in use. In a Maximum Megabytes of Physical RAM Available field, specify an amount of memory for use in parallel processing. As a rule of thumb, enter total RAM minus 8 GB; you may need to adjust this value if other processes run slowly.

- Enforce Allocated Analysis Time Per Filter: Select this check box, and enter a number in the Minutes field, to limit the time that transaction models and controls can run.

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

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

Language Preferences

In the Language Preferences section, choose languages in which GRC users may work. Select their check boxes, then select Actions > Save. "English (U.S.)" should be selected by default; do not deselect it. Once selected here, languages are available to administrators as they create GRC user accounts, or to GRC users as they set user preferences.

Schema Import/Export

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 *Enterprise 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 *Enterprise 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 the Schema Import/Export section, click the Download button.

2. An Information pop-up window opens, identifying a job number. Note the number, then close the window (click on its OK button).

3. Using the Navigator, go to Tools > Setup and Administration > Manage Jobs (see page 9-1). In the Manage Jobs page, locate the row displaying the job ID you noted in step 2. Click on the link in its Message cell.

4. A Job Detail window opens. In it, click on the Item Results link.

5. A file-download window offers you options to open or save the export file. The precise behavior of this window depends on the web browser you use, but in general, select the Save option and, in a distinct save-as dialog, navigate to the folder in which you want to save the file.

6. Close the Job Detail window (click on its OK button).

To upload a schema:

1. Ensure that an empty schema, and a tablespace for it, are created on the database server. (See the *Enterprise Governance, Risk and Compliance Installation Guide*.)

2. In the Schema Import/Export section, 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 are not changed subsequently. See the *Enterprise 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. A value greater that 21 is recommended. To prevent passwords from expiring, set this value to 10000.

A PASSWORD_EXPIRATION_MESSAGE job runs daily. It tracks users whose passwords will expire within three weeks, and, if notifications have been configured (see page 5-6), sends each user warning messages by email at weekly intervals. Messages are sent to the address recorded for each user in the Email Address 1 field of the Create User page (see page 3-6). A user can respond to such a message by logging on to GRC and using the Preferences page (see page 1-7) to change his password.

- 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 5-5).

- 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.

    (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. See page 1-4 for more on worklists.)

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 GRC 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 *Enterprise 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 *Enterprise Governance, Risk and Compliance Installation Guide*. (Also, see the discussion of the Use Basic Authentication for Web Service field on page 5-5.)

Configuring Notifications

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

GRC can alert result investigators not only when CCM 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 GRC 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.

    – Password: The password with which one would log on to the SMTP server.

    – Confirm Password: The SMTP server password entered in the Password field.

    – 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 the check box to allow GRC to access the SMTP server through secure sockets layer (SSL). The SMTP server must be configured to support SSL.

    – Enable Notification: Select this check box to activate the sending of work-list 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.

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

Purging Incidents

Ordinarily, records of CCM incidents remain in the Incident Management page even after they have reached an end status (Resolved, Control Inactive, or Closed). The potential exists for the number of incidents available for viewing to become large and unwieldy. 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 the CCM module, not to EGRCM (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.

6

Application Datasources and Libraries

Use the Manage Application Datasources page to set up Oracle EBS, PeopleSoft, and other datasources for use with AACG or ETCG, and to synchronize data for those datasources: 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 for use in CCM models and controls, or connectors to link GRC to datasources other than Oracle EBS or PeopleSoft: Select Setup and Administration under Tools in the Navigator, then Manage Application Libraries under Setup.

Both of these pages apply to the CCM module. If you use EGRCM 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.

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 or PeopleSoft.

   • Application Type Version: Select the version number of the business-management application to which you are connecting.

   • Default Datasource: Select the checkbox to make the datasource you are configuring the default for use in transaction models. Only one datasource can have this value selected.

- Connector Type: For an Oracle EBS or PeopleSoft datasource, select Default. For any other application, you would need to have created and uploaded a custom connector (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.

  – Password: For Oracle EBS or PeopleSoft, enter the password for the business-application database.

  – Port: For Oracle EBS or PeopleSoft, enter the port number that the business-application database uses to communicate with other applications.

  – Service Name: For Oracle EBS or PeopleSoft, supply the SID value configured for the business-application database in the tnsnames.ora file.

  – Username: For Oracle EBS or PeopleSoft, supply the user name for the business-application database. (For an Oracle database, this is the same as Schema Name; for an Oracle EBS instance, this is typically APPS.)

  – Password: For Oracle EBS or PeopleSoft, supply the password that authenticates the user name for the business-application database.

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

To ensure CCM models and controls evaluate current data, run synchronization — a process that copies data from datasources (business applications) to GRC.

For ETCG only, a Graph Synchronization Date Limit (if enabled in the Properties tab of the Manage Application Configurations page) causes the synchronization of certain frequently modified business objects to operate only on records created or updated in datasources on or after a specified date. See page 5-2 for a complete description of this feature.

To synchronize data manually:

1. In the Manage Application Datasources page, select the row for the datasource with which you want to synchronize data.

2. Do either of the following:

- Click on Actions > Synchronize Transaction. This causes data for business objects used in existing ETCG models and controls to be synchronized once,

immediately. (Before you can synchronize transaction data, at least one transaction model must exist.)

- Click on Actions > Synchronize Access. This causes all data used by AACG to be synchronized once, immediately. (You can synchronize access data even if no access models or controls exist.)

3. A message presents a job number. Note the number, then close the message (click on its OK button).

4. To check on the status of the synchronization job, navigate to Tools > Setup and Administration > Manage Jobs (see page 9-1). In the Manage Jobs page, locate the row displaying the job ID you noted in step 3. Click on the link in its Message cell. (Note: You can use the distinct Manage CCM Jobs page instead, but the Manage Jobs page may be better suited to this task.)

Alternatively, you can schedule synchronization jobs to be run:

1. In the Manage Application Datasources page, select the row for the datasource with which you want to synchronize data.

2. Click on Actions > Schedule Synchronize. 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

3. To track the scheduled synchronization runs, navigate to Tools > Setup and Administration > Manage Scheduling (see page 9-3).

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.

An ordinary synchronization run is incremental — it creates or updates only records that are new or have changed since the previous synchronization. For an ETCG datasource, you can instead "rebuild the graph" — delete all data for a given datasource and replace it with a complete set of current data. This typically takes longer than an ordinary synchronization, and it potentially has a significant effect on existing incidents, model results, and worklists. As a result, a graph rebuild should not be performed frequently. To rebuild the graph, select the row for a datasource, select Actions > Rebuild Graph, and click the OK button in a confirmation message that appears.

Uploading Business Objects

As you create CCM 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, 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 a import 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.

7

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, content types, and installation options apply both to AACG, ETCG, 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.

See Appendix A for definitions of seeded lookup values.

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 do two things: First, you can specify the currency used by an EGRCM installation. (Only one currency is supported throughout the installation.) In the Installation Currency section of the page, select the currency you want to use in the Currency list box.

Second, you can customize the application "branding" — the logo and product name displayed on each GRC page. By default, GRC displays the Oracle logo and the name "Enterprise Governance, Risk and Compliance."

To retain the default values, ensure that the Use Oracle Branding check box remains selected in the Application Branding section of the page. (It is selected by default.)

To change the branding:

1. Clear the Use Oracle Branding check box. (Other branding fields are inactive until you do so.)

2. In the Branding Logo field, click on the Browse button, then navigate to the image file you want to use as a logo. The size of the image must be 119 × 25 pixels, and the file must be in Portable Graphics (.png) format. When you select the file, its name is displayed in the Branding Logo field, and the image appears to the right of the field.

3. Type a product name in the Sub-branding Text field. The maximum length of the name is 30 characters.

When you finish selecting a currency, customizing branding, or both, click the Save button.

For branding changes to take effect, restart the application server (WebLogic or Tomcat, depending on your installation), and instruct each user to clear the cache of the web browser in which he or she works with GRC.

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.

8

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.

So, most module-management functionality applies to only to EGRCM. One exception is Manage Module Perspectives (page 8-4). In any GRC application, 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 8-5), which you can use to import perspectives for use with AACG or ETCG, and all types of operational data for EGRCM.

Managing Modules

Use the Manage Modules page to create a custom module. To do so is to select the base, risk, and control objects the module is to contain, and to define parent/child relationships among them.

The standard template (the only one delivered with GRC) makes six base objects, ten risk objects, and ten control objects available. (Each of these is initially labeled with a letter of the alphabet, although you can rename them.) Additionally, one issue object and one remediation plan object are automatically selected for use throughout the module. One event object and one consequence object are also available automatically; in the Configure Module Objects page (page 8-2), they may be associated with any number of risk objects selected for the module.

In general, a base object can be the parent of a risk or a control, and a risk can be the parent of a control. A base object can also be the parent of base objects that follow it alphabetically. However, there are special cases:

- Base Object E may be the parent of a control, but the child of a risk.

- Base Object F may be the child of a control.

- Risk Object A may be a parent to Risk Object H, B to I, and C to J.

- Control Object A may be a parent to Control Object H, B to I, and C to J.

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. Each time you select an object, check boxes labeled with the name of the new object may appear in the squares representing objects you've already selected. You can select a check box to designate an object as a child of the object in which the check box appears. Or you can clear a check box to a sever a relationship between objects.

    For example, suppose you select Base Object A, Risk Object A, and Control Object A. The square representing Base Object A contains check boxes labeled Risk Object A and Control Object A, so there is the opportunity to designate the base object as a "parent" of the risk and control objects.

    The square representing Risk Object A contains a check box labeled Control Object A, so there is an opportunity to designate risk as a parent of control, but no opportunity to designate risk as a parent of base object. The square representing Control Object A contains no check boxes; it cannot be the parent of any object.

    Suppose further that in the square representing Base Object A, you select the Risk Object A check box but clear the Control Object A check box. Then, in the square representing Risk Object A, you select the Control Object A check box. The base object is therefore the parent of the risk object, the risk object is the parent of the control object, and there is no direct relationship between the base object and the control object.

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.

- Issue: Determines whether an Issues tab appears in the Manage page for an object. Select Show (the default) or Hide. This option applies to base objects, risks, and controls in modules other than Financial Governance.

- 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. Select the Manage Module Perspectives entry under Module Management in the Setup and Administration tasks.

2. In the Manage Module Perspectives page, click on the module for which you want to associate perspectives with objects, and then select Actions > Edit.

3. A page opens for the module you've selected. In it, choose Actions > Create.

4. 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.

5. 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 Manager 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 without data, with all data, or with perspective data. If you choose a with-data option, the template contains operational data already configured for the module. (The export of this template is completed in the GRC Manage Jobs page; see page 9-2.)

• 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.

9

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.

GRC provides two pages in which users may mange jobs: view job status, manage exported and imported data, cancel jobs, or purge job history.

- A general-purpose Manage Jobs page provides a listing for every job that is run on GRC. To open this page, select Setup and Administration under Tools in the GRC Navigator, then select Manage Jobs under Administration in the Tasks list.

- A Manage CCM Jobs page is filtered to present listings only for jobs that analyze models or continuous controls in the CCM module. To open this page, select Continuous Control Management under Continuous Monitoring in the GRC Navigator, then select Manage CCM Jobs under Control Administration in the Tasks list.

The Manage CCM Jobs page offers search capability (see "Searching Among Records," page 1-5), with which users may refilter the page to display any sort of job. The general-purpose Manage Jobs page does not offer search capability. Otherwise, the two pages offer the same functionality.

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: For a control- or model-analysis job, the name of the control or model that has been analyzed (if the job focuses on only one control or model) or a message indicating that multiple controls or models have been analyzed.

  For any other sort of job, a plain-language description of what the job does.

- Type: An internal code identifying 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 a job finishes 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).

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

Managing Export and Import 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 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 8-5. 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 Item Results link.

4. A file-download window offers you options to open or save the export file. The precise behavior of this window depends on the web browser you use, but in general, select the Save option and, in a distinct save-as dialog, navigate to the 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 GRC 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.

A

Appendix: Seeded Lookups

For each list of values in GRC, a lookup table stores the values from which a user may select (see "Managing Lookup Tables," page 7-1). In each case, 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 appears in an LOV. Each entry may also have a description.

The following lookup values are seeded with GRC.

BIP_EXPRESSION Lookup Type

Lookup Code	Meaning	Description
CURRENTDATE	Current Date	Current Date

BIP_PARAM_TYPE Lookup Type

Lookup Code	Meaning	Description
EXPRESSION	Expression	Expression
TEXT	Text	Text
COMPATTR	Component Attribute	Component Attribute

BIP_REPORT_HEADER Lookup Type

Lookup Code	Meaning	Description
NHNP	No header and no parameters	No header and no parameter
NP	No parameters	No parameter
SH	Show header and filer	Show header and filer
NH	No header	No header

BO_ADMIN_STATE Lookup Type

Lookup Code	Meaning	Description
151	Created	Created
152	Mapped	Mapped
153	Formatted	Formatted

BO_ADMIN_STATUS Lookup Type

Lookup Code	Meaning	Description
161	Completed	Completed
162	Processing	Processing
163	Error	Error

BO_ADMIN_TYPE Lookup Type

Lookup Code	Meaning	Description
141	Dictionary	Dictionary
142	Mapping	Mapping

DATE_FORMAT Lookup Type

Lookup Code	Meaning	Description
M-d-yy	(1-31-09)	(1-31-09)
yyyy/MM/dd	(2009/01/31)	(2009/01/31)
M.d.yy	(1.31.09)	(1.31.09)
M.d.yyyy	(1.31.2009)	(1.31.2009)
M/d/yy	(1/31/09)	(1/31/09)
M/d/yyyy	(1/31/2009)	(1/31/2009)
MM-dd-yy	(01-31-09)	(01-31-09)
MM-dd-yyyy	(01-31-2009)	(01-31-2009)
MM.dd.yy	(01.31.09)	(01.31.09)
MM.dd.yyyy	(01.31.2009)	(01.31.2009)
MM/dd/yy	(01/31/09)	(01/31/09)
MM/dd/yyyy	(01/31/2009)	(01/31/2009)
d-M-yy	(31-1-09)	(31-1-09)
d-M-yyyy	(31-1-2009)	(31-1-2009)
d.M.yy	(31.1.09)	(31.1.09)
d.M.yyyy	(31.1.2009)	(31.1.2009)
d/M/yy	(31/1/09)	(31/1/09)
d/M/yyyy	(31/1/2009)	(31/1/2009)

Lookup Code	Meaning	Description
dd-MM-yy	(31-01-09)	(31-01-09)
dd-MM-yyyy	(31-01-2009)	(31-01-2009)
dd.MM.yy	(31.01.09)	(31.01.09)
dd.MM.yyyy	(31.01.2009)	(31.01.2009)
dd/MM/yy	(31/01/09)	(31/01/09)
dd/MM/yyyy	(31/01/2009)	(31/01/2009)
yy-M-d	(09-1-31)	(09-1-31)
yy-MM-dd	(09-01-31)	(09-01-31)
yy. M. d	(09. 1. 31)	(09. 1. 31)
yy.M.d	(09.1.31)	(09.1.31)
yy.MM.dd	(09.01.31)	(09.01.31)
yy/M/d	(09/1/31)	(09/1/31)
yy/MM/dd	(09/01/31)	(09/01/31)
yyyy-M-d	(2009-1-31)	(2009-1-31)
yyyy-MM-dd	(2009-01-31)	(2009-01-31)
yyyy.M.d	(2009.1.31)	(2009.1.31)
yyyy.MM.dd	(2009.01.31)	(2009.01.31)
yyyy/M/d	(2009/1/31)	(2009/1/31)
M-d-yyyy	(1-31-2009)	(1-31-2009)

ENTITLEMENT_STATUS Lookup Type

Lookup Code	Meaning	Description
INACTIVE	Inactive	Inactive
ACTIVE	Active	Active

ERP_DB_TYPE Lookup Type

Lookup Code	Meaning	Description
171	MS SQLServer	MS SQLServer
172	DB2	DB2
173	Oracle	Oracle

GRCC_CONTROL_ENFORCEMENT_TYPE Lookup Type

Lookup Code	Meaning	Description
4	Approval Required	Approval Required
3	Prevent	Prevent
1	Monitor	Monitor

GRCC_CONTROL_STATE Lookup Type

Lookup Code	Meaning	Description
INVALID	Invalid	Invalid
APPROVED	Approved	Approved

GRCC_CONTROL_TYPE Lookup Type

Lookup Code	Meaning	Description
174	Transaction	Transaction
173	Access	Access

GRCC_INCIDENT_STATE Lookup Type

Lookup Code	Meaning	Description
IN_INVESTIGATION	In Investigation	In Investigation
APPROVED	Approved	Approved
CLOSED	Closed	Closed

GRCC_OBJECT_TYPE_CODE Lookup Type

Lookup Code	Meaning	Description
GRCC_CONTROL	Control	GRCC Control
GRCC_MODEL	Model	GRCC Model
GRCC_INCIDENT	Result	GRC Result

GRCM_CONTROL_ENFORCEMENT_TYPE Lookup Type

Lookup Code	Meaning	Description
DETECTIVE	Detective	Detective
CORRECTIVE	Corrective	Corrective
PREVENTIVE	Preventive	Preventive

GRCM_FLEX_OBJECT_CATEGORY Lookup Type

Lookup Code	Meaning	Description
FLEX_CONTROL_OBJECT	Control Object	Control Object
FLEX_RISK_OBJECT	Risk Object	Risk Object
FLEX_ISSUE_OBJECT	Issue Object	Issue Object
FLEX_BASE_OBJECT	Base Object	Base Object

GRCM_FLEX_OBJECT_TYPE Lookup Type

Lookup Code	Meaning	Description
27	Event And Consequence Object	Event And Consequence Object
28	Issue Object	Issue Object
5	Base Object E	Base Object E
6	Base Object F	Base Object F
7	Risk Object A	Risk Object A
8	Risk Object B	Risk Object B
9	Risk Object C	Risk Object C
10	Risk Object D	Risk Object D
11	Risk Object E	Risk Object E
12	Risk Object F	Risk Object F
13	Risk Object G	Risk Object G
14	Risk Object H	Risk Object H
15	Risk Object I	Risk Object I
16	Risk Object J	Risk Object J
17	Control Object A	Control Object A
18	Control Object B	Control Object B
19	Control Object C	Control Object C
20	Control Object D	Control Object D
21	Control Object E	Control Object E
22	Control Object F	Control Object F
23	Control Object G	Control Object G
24	Control Object H	Control Object H
25	Control Object I	Control Object I
26	Control Object J	Control Object J
1	Base Object A	Base Object A
2	Base Object B	Base Object B
3	Base Object C	Base Object C
4	Base Object D	Base Object D

GRCM_FLEX_TMPL_STRATEGY_STATUS Lookup Type

Lookup Code	Meaning	Description
ACTIVE	Active	Active
RETIRE	Inactive	Inactive

GRCM_FLEX_TMPL_STRATEGY_TYPE Lookup Type

Lookup Code	Meaning	Description
FLEX_TEMPLATE	Flex Template	Flex Template

GRCM_MODULE_TYPE Lookup Type

Lookup Code	Meaning	Description
FINANCIAL_GOVERNANCE	Financial Governance	Financial Governance

GRCM_OBJECT_ACCESS_TYPE Lookup Type

Lookup Code	Meaning	Description
GRCM_OBJECT_ACCESS_PRIVATE	PRIVATE	PRIVATE
GRCM_OBJECT_ACCESS_PUBLIC	PUBLIC	PUBLIC

GRCM_OBJECT_TYPE_CODE Lookup Type

Lookup Code	Meaning	Description
GRC_RISK_ANALYSIS	Risk Analysis	Risk Analysis
GRC_CONTROL	Control	Control
GRC_ASMT_PLAN	Assessment Plan	Assessment Plan
GRC_ASMT_TEMPLATE	Assessment Template	Assessment Template
GRC_ASMT_ASSESSMENT	Assessment	Assessment
GRC_ISSUE	Issue	Issue
GRC_REMED_PLAN	Remediation Plan	Remediation Plan
GRC_REMED_TASK	Remediation Task	Remediation Task
GRC_ACTION_ITEM	Action Item	Action Item
GRC_PROCESS	Process	Process
GRC_RISK_ANALYSIS_MODEL	Risk Analysis Model	Risk Analysis Model
GRC_CONSEQUENCE	Consequence	Consequence
GRC_EVENT	Event	Event
GRC_IMPACT_MODEL	Impact Model	Impact Model
GRC_LIKELIHOOD_MODEL	Likelihood Model	Likelihood Model
GRC_PROPOSED_RISK	Proposed Risk	Proposed Risk
GRC_RISK_CONTEXT_MODEL	Risk Context Model	Risk Context Model
GRC_RISK_SIG_MODEL	Risk Significance Model	Risk Significance Model
GRC_TREATMENT	Treatment	Treatment

Lookup Code	Meaning	Description
GRC_TEST_PLAN	Test Plan	Test Plan
GRC_PERSPECTIVE_ TREE	Perspective Tree	Perspective Tree
GRC_TEST_ INSTRUCTION	Test Instruction	Test Instruction
GRC_PERSP_ITEM	Perspective Item	Perspective Item
GRC_SURVEY_ TEMPLATE	Survey Template	Survey Template
GRC_ASMT_RISK_ RESULT	Assessment Risk Result	Assessment Risk Result
GRC_ASMT_CONTROL _RESULT	Assessment Control Result	Assessment Control Result
GRC_ASMT_PROCESS _RESULT	Assessment Process Result	Assessment Process Result
GRC_TREATMENT_PLAN	Treatment Plan	Treatment Plan
GRC_RISK_EVAL	Risk Evaluation	Risk Evaluation
GRC_RISK	Risk	Risk
GRC_SURVEY	Survey	Survey
GRC_ASMT_PERSP_ RESULT	Assessment Perspective Item Result	Assessment Perspective Item Result

GRCM_OBJECT_TYPE_UDA_LIST Lookup Type

Lookup Code	Meaning	Description
GRC_RISK_ANALYSIS	Risk Analysis	Risk Analysis
GRC_RISK	Risk	Risk
GRC_ASMT_ASSESSMENT	Assessment	Assessment
GRC_ISSUE	Issue	Issue
GRC_REMED_PLAN	Remediation Plan	Remediation Plan
GRC_REMED_TASK	Remediation Task	Remediation Task
GRC_ACTION_ITEM	Action Item	Action Item
GRC_PROCESS	Process	Process
GRC_CONSEQUENCE	Consequence	Consequence
GRC_EVENT	Event	Event
GRC_PROPOSED_RISK	Proposed Risk	Proposed Risk
GRC_RISK_CONTEXT_ MODEL	Risk Context Model	Risk Context Model
GRC_TREATMENT	Treatment	Treatment
GRC_TREATMENT_PLAN	Treatment Plan	Treatment Plan
GRC_TEST_PLAN	Test Plan	Test Plan
GRC_TEST_INSTRUCTION	Test Instruction	Test Instruction
GRC_PERSP_ITEM	Perspective Item	Perspective Item

Lookup Code	Meaning	Description
GRC_RISK_EVAL	Risk Evaluation	Risk Evaluation
GRC_CONTROL	Control	Control

GRCM_PERSPECTIVE_TYPE Lookup Type

Lookup Code	Meaning	Description
GRC_PERSP_CCMTYPE	Continuous Control Monitoring Type	Continuous Control Monitoring Type
GRC_PERSP_DATASOURCE	Data Source	Data Source
GRC_PERSP_BUSINESS_OBJECT	Business Object	Business Object
GRC_PERSP_ORG	Organization	Organization Perspective
GRC_PERSP_FIN_ACCT	Financial Governance Accounts	Financial Governance Accounts Perspective
GRC_PERSP_LAW_REG	Laws and Regulations	Laws and Regulations Perspective
GRC_PERSP_FLEX	Flex Template Module	Flex Template Module
GRC_PERSP_STD_FWK	Standards and Framework	Standards and Framework Perspective
GRC_PERSP_ACTIVITY	Activity	Activity Perspective
GRC_PERSP_CCM_PARTICIPANT_GROUP	Participant Group	Participant Group
GRC_PERSP_BUSINESS_PROCESS	Business Process	Business Process
GRC_PERSP_CCM_RISK_TYPE	Risk	Risk
GRC_PERSP_MJR_PROC	Major Process	Major Process Perspective

GRCM_WORKLIST_TYPE_CODE Lookup Type

Lookup Code	Meaning	Description
GRC_REVIEW	Review	Review
GRC_INVESTIGATE	Investigate	Investigate
GRC_DRAFT	Draft	Draft
GRC_NOTIFY	Notify	Notify
GRC_ASSIGNTODFT_TASK	Assign To Draft	Assign To Draft
GRC_FYI_TASK	For Your Information	For Your Information
GRC_UPSTREAM_FYI	Upstream FYI	Upstream FYI
GRC_ISSUES_DRAFT	Issues Draft	Issues Draft
GRC_PRISK_DRAFT	Propose Risk Draft	Propose Risk Draft
GRC_PRISK_FYI	Propose Risk FYI	Propose Risk FYI

Lookup Code	Meaning	Description
GRC_ASMT_RESULT	Complete Assessment	Complete Assessment
GRC_SURVEY_COMPLETE	Complete Survey	Complete Survey
GRC_INFO_REQUESTED	Information Requested	Information Requested
GRC_RISK_ANALYSIS_ COMPLETE	Complete Risk Analysis	Complete Risk Analysis
GRC_RISK_EVALUATION_ COMPLETE	Complete Risk Evaluation	Complete Risk Evaluation
GRC_ACTION_ITEM_ COMPLETE	Complete Action Item	Complete Action Item
GRC_CLOSED_REVIEW	Closed-In Review	Closed-In Review
GRC_CLOSED_APPROVE	Closed-In Approve	Closed-In Approve
GRC_CLOSED_INFO_ REQUESTED	Closed-In Information Requested	Closed-In Information Requested
GRC_COMPLETED_REVIEW	Completed-In Review	Completed-In Review
GRC_COMPLETED_APPROVE	Completed-In Approve	Completed-In Approve
GRC_COMPLETED_INFO_ REQUESTED	Completed-In Information Requested	Completed-In Information Requested
GRC_REPORTED_ISSUES_ DRAFT	Reported Issue	Reported Issue
GRC_REJECTED_DRAFT	Rejected Draft	Rejected Draft
GRC_REPORTED_PRISK_ DRAFT	Reported Propose Risk Draft	Reported Propose Risk Draft
GRC_REJECTED_ISSUES_ DRAFT	Rejected Issue Draft	Rejected Issue Draft
GRC_REJECTED_ASMT_ RESULT	Complete Rejected Assessment	Complete Rejected Assessment
GRC_APPROVE	Approve	Approve

GRC_ACTION_ITEM Lookup Type

Lookup Code	Meaning	Description
COMPLETE	Complete	Complete
ACTIVE	Active	Active

GRC_ACTION_ITEM_PRIORITY Lookup Type

Lookup Code	Meaning	Description
MEDIUM	Medium	Medium
LOW	Low	Low
HIGH	High	High

GRC_ACTION_ITEM_PROGRESS Lookup Type

Lookup Code	Meaning	Description
ASSIGNED	Assigned	Assigned
DELAYED	Delayed	Delayed
BLOCKED	Blocked	Blocked
COMPLETED	Completed	Completed
ON_TARGET	On Target	On Target

GRC_ACTION_ITEM_PROGRESS_GRAPH Lookup Type

Lookup Code	Meaning	Description
COMPLETION	Completion	Completion

GRC_ANALYSIS_TIME_PERIOD Lookup Type

Lookup Code	Meaning	Description
WEEK	Week	Per Week
CENTURY	Century	Per Century
DECADE	Decade	Per Decade
YEAR	Year	Per Year
QUARTER	Quarter	Per Quarter
MONTH	Month	Per Month
DAY	Day	Per Day

GRC_APPLICATION_MODULE Lookup Type

Lookup code	Meaning	Description
REVIEW	In Review	In Review
RETIRE	Inactive	Inactive
NEW	New	New
APPROVE	Awaiting Approval	Awaiting Approval
PROCESSING	Work In Progress	Work In Progress
ACTIVE	Active	Active
RETIRE_REVIEW	In Review	In Review
RETIRE_APPROVE	Awaiting Approval	Awaiting Approval

GRC_APPROVAL_STATE Lookup Type

Lookup Code	Meaning	Description
APPROVAL	In approval	In approval
ACTIVE	Active	Active
REVIEW	In review	In review
SUBMIT	Submitted	Submitted
WITHDRAW	Withdrawn	Withdrawn
REJECT	Rejected	Rejected

GRC_APPROVE_ACTION Lookup Type

Lookup Code	Meaning	Description
REJECT	Reject	Rejected
RETURN	Return for information	Return for more information
APPROVE	Approve	Approval complete

GRC_ASMT_ADHOCPLAN Lookup Type

Lookup Code	Meaning	Description
ADHOC	Adhoc	Adhoc

GRC_ASMT_ASSESSMENT Lookup Type

Lookup Code	Meaning	Description
REVIEW	In Review	In Review
ACTIVE	Active	Active
PROCESSING	Work In Progress	Work In Progress
APPROVE	Awaiting Approval	Awaiting Approval
CLOSED	Closed	Closed
NEW	New	New

GRC_ASMT_DFLT_PLANNAMES Lookup Type

Lookup Code	Meaning	Description
ADHOC	Adhoc	Adhoc

GRC_ASMT_GRID_RSLT_CAT Lookup Type

Lookup Code	Meaning	Description
COMPLETED	Completed	Completed
INPROGRESS	Current	Current
PAST_DUE	Overdue	Overdue

GRC_ASMT_GRID_RSLT_CATRO Lookup Type

Lookup Code	Meaning	Description
INPROGRESS	Current	Current
PAST_DUE	Overdue	Overdue

GRC_ASMT_PLAN Lookup Type

Lookup Code	Meaning	Description
RETIRE_REVIEW	In Review	In Review
RETIRE_APPROVE	Awaiting Approval	Awaiting Approval
REVIEW	In Review	In Review
APPROVE	Awaiting Approval	Awaiting Approval
RETIRE	Inactive	Inactive
PROCESSING	Work In Progress	Work In Progress
NEW	New	New
ACTIVE	Active	Active

GRC_ASMT_PLAN_STATE Lookup Type

Lookup Code	Meaning	Description
NEW	New	New
REVIEW	In Review	In Review
EDIT	In Edit	In Edit
ADDL_INFO_REVIEW	Request for Information In Review	Request for Information In Review
ADDL_INFO_APPROVE	Request for Information In Approval	Request for Information In Approval
REJECTED	Rejected	Rejected
APPROVE	Awaiting Approval	Awaiting Approval
APPROVED	Approved	Approved

GRC_ASMT_RESULT Lookup Type

Lookup Code	Meaning	Description
REJECTED	Rejected	Rejected
ADDL_INFO_APPROVE	Request for Information In Approval	Request for Information In Approval
ADDL_INFO_REVIEW	Request for Information In Review	Request for Information In Review
REVIEW	In Review	In Review
APPROVE	Awaiting Approval	Awaiting Approval
NEW	Active - New	Active - New
APPROVED	Approved	Approved
ACTIVE	Active	Active
COMPLETED	Completed	Completed

GRC_ASMT_SELCRIT Lookup Type

Lookup Code	Meaning	Description
NO_CRITERIA	No Criteria	No Criteria

GRC_ASMT_SELCRIT_CTRLSCOPE Lookup Type

Lookup Code	Meaning	Description
ASSESSMENT	Assessment	Assessment
AUDIT	Audit	Audit

GRC_ASMT_SELCRIT_CTRLSTRAT Lookup Type

Lookup Code	Meaning	Description
MITIGATING	Mitigating	Mitigating
MONITORING	Monitoring	Monitoring
NONE	None	None
KEY	Key	Key
OTHER	Other	Other
COMPENSATING	Compensating	Compensating
REDUNDANT	Redundant	Redundant

GRC_ASMT_SELCRIT_OPERATORS Lookup Type

Lookup Code	Meaning	Description
<>	not equal to	not equal to
=	equal to	equal to
ENDSWITH	ends with	ends with
ISBLANK	is blank	is blank
ISNOTBLANK	is not blank	is not blank
STARTSWITH	starts with	starts with
CONTAINS	contains	contains

GRC_ASMT_SELCRIT_STATE Lookup Type

Lookup Code	Meaning	Description
APPROVED	Approved	Approved
APPROVE	Awaiting Approval	Awaiting Approval
ADDL_INFO_APPROVE	Request for Information In Approval	Request for Information In Approval
ADDL_INFO_REVIEW	Request for Information In Review	Request for Information In Review
REVIEW	In Review	In Review
EDIT	In Edit	In Edit

GRC_ASMT_STATUS Lookup Type

Lookup Code	Meaning	Description
CURRENT	Current	Current
COMPLETE	Complete	Complete
OVERDUE	Overdue	Overdue

GRC_ASMT_TEMPLATE Lookup Type

Lookup Code	Meaning	Description
APPROVE	Awaiting Approval	Awaiting Approval
RETIRE	Inactive	Inactive
NEW	New	New
PROCESSING	Work In Progress	Work In Progress
REVIEW	In Review	In Review
RETIRE_APPROVE	Awaiting Approval	Awaiting Approval
RETIRE_REVIEW	In Review	In Review
ACTIVE	Active	Active

GRC_ASMT_TEMPLATE_STATE Lookup Type

Lookup Code	Meaning	Description
NEW	New	New
REVIEW	In Review	In Review
EDIT	In Edit	In Edit
ADDL_INFO_REVIEW	Request for Information In Review	Request for Information In Review
ADDL_INFO_APPROVE	Request for Information In Approval	Request for Information In Approval
APPROVED	Approved	Approved
APPROVE	Awaiting Approval	Awaiting Approval
REJECTED	Rejected	Rejected

GRC_ASMT_VIEW_BY Lookup Type

Lookup Code	Meaning	Description
MY_ACTIVITIES	My Activities	My Activities
ACTIVITIES_OVERVIEW	Activity Overview	Activity Overview

GRC_ASSESSMENT_TYPE Lookup Type

Lookup Code	Meaning	Description
FINANCIAL_YEAR_END	Financial Year End	Financial Year End
FINANCIAL_SOD	Financial SOD	Financial SOD

GRC_ATTACHMENT_TYPE Lookup Type

Lookup Code	Meaning	Description
URL	URL	URL
DESKTOP_FILE	Desktop File	Desktop File

GRC_BUSINESS_ENTITY_ACTION Lookup Type

Lookup Code	Meaning	Description
SAVE	Save	Save
SUBMIT	Submit	Submit
WITHDRAW	Withdraw	Withdraw
REPLY	Respond to Request for Information	Respond to Request for Information
MARK_COMPLETE	Mark Complete	Mark Complete

Lookup Code	Meaning	Description
ACCEPT	Accept	Accept
REJECT	Reject	Reject
CLOSE	Close	Close
ADDITIONAL_INFO	Request for Additional Information	Request for Additional Information

GRC_BUSINESS_ENTITY_STATE Lookup Type

Lookup Code	Meaning	Description
OPEN	Open	Open
COMPLETED	Completed	Completed
REPORTED	Reported	Reported
CLOSED_REVIEW	Closed – In Review	Closed – In Review
CLOSED_ADDL_INFO_ REVIEW	Closed – Request For Information In Review	Closed – Request For Information In Review
CLOSED_ADDL_INFO_ APPROVE	Closed – Request For Information In Approval	Closed – Request For Information In Approval
CLOSED_APPROVE	Closed – Awaiting Approval	Closed – Awaiting Approval
CLOSED	Closed	Closed
FINAL_CLOSE	Final Close	Final Close
COMPLETED_REVIEW	Completed Review	Completed Review
COMPLETED_APPROVE	Completed Approval	Completed Approval
COMPLETED_ADDL_ INFO_REVIEW	Completed – Request for Information In Review	Completed – Request for Information In Review
COMPLETED_ADDL_ INFO_APPROVE	Completed – Request for Information In Approval	Completed – Request for Information In Approval
IN_INVESTIGATION	In Investigation	In Investigation
DECLINED	Declined	Declined
PARTIALLY_COMPLETED	Partially Complete	Partially Complete
ACTIVE	Active	Active
APPROVED	Approved	Approved
APPROVE	Awaiting Approval	Awaiting Approval
REJECTED	Rejected	Rejected
ADDL_INFO_APPROVE	Request for Information In Approval	Request for Information In Approval
ADDL_INFO_REVIEW	Request for Information In Review	Request for Information In Review
EDIT	In Edit	In Edit
CANCELLED	Cancelled	Cancelled
NEW	New	New
REVIEW	In Review	In Review

GRC_BUSINESS_ENTITY_STATUS Lookup Type

Lookup Code	Meaning	Description
INACTIVE	Inactive	Inactive
ACTIVE	Active	Active

GRC_BUS_ENTITY_MODEL_STATUS Lookup Type

Lookup Code	Meaning	Description
RETIRE_REVIEW	In Review	In Review
REVIEW	In Review	In Review
RETIRE	Inactive	Inactive
ACTIVE	Active	Active
NEW	New	New
RETIRE_APPROVE	Awaiting Approval	Awaiting Approval
PROCESSING	Work In Progress	Work In Progress
APPROVE	Awaiting Approval	Awaiting Approval

GRC_CALENDAR_TYPE Lookup Type

Lookup Code	Meaning	Description
M	Monthly	Calendar that is divided into 12 calendar periods
Q	Quarterly	Calendar that is divided into 4 quarterly periods
A	Annual	Calendar that represents one period for the year

GRC_CMS_CONNECTION_TYPE Lookup Type

Lookup Code	Meaning	Description
DB	Database	Database Connection
WS	Web Service	Web Service Connection

GRC_CMS_DIRECTION_INFO Lookup Type

Lookup Code	Meaning	Description
PUSH_TO_SYSTEM	Push to System	Push to System
PULL_FROM_SYSTEM	Pull from System	Pull from System

GRC_CONSEQUENCE Lookup Type

Lookup Code	Meaning	Description
APPROVE	Awaiting Approval	Awaiting Approval
ACTIVE	Active	Active
NEW	New	New
NONE	None	None
PROCESSING	Work In Progress	Work In Progress
RETIRE_APPROVE	Awaiting Approval	Awaiting Approval
RETIRE_REVIEW	In Review	In Review
REVIEW	In Review	In Review
RETIRE	Inactive	Inactive

GRC_CONSEQUENCE_STATUS Lookup Type

Lookup Code	Meaning	Description
DRAFT	Draft	Draft
NEW	New	New

GRC_CONTENT_TYPE Lookup Type

Lookup Code	Meaning	Description
OTHER	Other	Other
TESTING_EVIDENCE	Testing Evidence	Testing Evidence
AUDIT_PAPER	Audit Paper	Audit Paper
PROCESS_FLOW	Process Flow	Process Flow
PROCESS_NARRATIVE	Process Narrative	Process Narrative

GRC_CONTROL Lookup Type

Lookup Code	Meaning	Description
RETIRE	Inactive	Inactive
REVIEW	In Review	In Review
RETIRE_REVIEW	In Review	In Review
RETIRE_APPROVE	Awaiting Approval	Awaiting Approval
APPROVE	Awaiting Approval	Awaiting Approval
NEW	New	New
PROCESSING	Work In Progress	Work In Progress
ACTIVE	Active	Active

GRC_CONTROL_AUDIT Lookup Type

Lookup Code	Meaning	Description
AICPA	AICPA	AICPA
PWC	PWC	PWC

GRC_CONTROL_FREQUENCY Lookup Type

Lookup Code	Meaning	Description
MONTHLY	Monthly	Monthly
DAILY	Daily	Daily
WEEKLY	Weekly	Weekly
YEARLY	Yearly	Yearly

GRC_CONTROL_METHOD Lookup Type

Lookup Code	Meaning	Description
MANUAL	Manual	Manual
AUTOMATIC	Automatic	Automatic

GRC_CONTROL_STATE Lookup Type

Lookup Code	Meaning	Description
REJECTED	Rejected	Rejected
APPROVE	Awaiting Approval	Awaiting Approval
APPROVED	Approved	Approved
ADDL_INFO_REVIEW	Request for Information In Review	Request for Information In Review
EDIT	In Edit	In Edit
REVIEW	In Review	In Review
ADDL_INFO_APPROVE	Request for Information In Approval	Request for Information In Approval
NEW	New	New

GRC_CONTROL_STATUS Lookup Type

Lookup Code	Meaning	Description
INACTIVE	Inactive	Inactive
ACTIVE	Active	Active

GRC_CORE_TYPE Lookup Type

Lookup Code	Meaning	Description
GRC_PROCESS	Process	Process
GRC_RISK	Risk	Risk
GRC_CONTROL	Control	Control

GRC_CTRL_ASSERTIONS Lookup Type

Lookup Code	Meaning	Description
VALUATION_ALLOCATION	Valuation or Allocation	Valuation or Allocation
RIGHTS_AND_OBLIGATIONS	Rights and Obligations	Rights and Obligations
PRESENTATION_DISCLOSURE	Presentation and Disclosure	Presentation and Disclosure
COMPLETENESS	Completeness	Completeness
EXISTENCE_OCCURRENCE	Existence or Occurrence	Existence or Occurrence

GRC_DELEGATE_OUTCOME Lookup Type

Lookup Code	Meaning	Description
Inactive	Inactive	Inactive

GRC_EVENT Lookup Type

Lookup Code	Meaning	Description
NEW	New	New
ACTIVE	Active	Active
RETIRE	Inactive	Inactive
PROCESSING	Work In Progress	Work In Progress
APPROVE	Awaiting Approval	Awaiting Approval
RETIRE_REVIEW	In Review	In Review
RETIRE_APPROVE	Awaiting Approval	Awaiting Approval
REVIEW	In Review	In Review

GRC_IMPACT_MODEL_TYPE Lookup Type

Lookup Code	Meaning	Description
SQUAN	Semi-Quantitative	Semi-Quantitative Analysis
QUAL	Qualitative	Qualitative Analysis

GRC_INCIDENT_STATUS Lookup Type

Lookup Code	Meaning	Description
REMEDIATION	Remediation	Remediation
CLOSED	Closed	Closed
RESOLVED	Resolved	Resolved
ACCEPTED	Accepted	Accepted
AUTHORIZED	Authorized	Authorized
ASSIGNED	Assigned	Assigned
CONTROL_INACTIVE	Control Inactive	Control Inactive

GRC_INCLUDE_EXCLUDE Lookup Type

Lookup Code	Meaning	Description
EXCLUDE	Exclude	Exclude
INCLUDE	Include	Include

GRC_ISSUE Lookup Type

Lookup Type	Meaning	Description
OPEN	Open	Open
REMEDIATE	In Remediation	In Remediation
CLOSE	Closed	Closed
HOLD	Hold for Future	Hold for Future
APPROVE	Awaiting Approval	Awaiting Approval
REPORTED	Reported	Reported
PROCESSING	Work in Progress	Work in Progress
REVIEW	In Review	In Review
NEW	New	New

GRC_ISSUE_ACTION Lookup Type

Lookup Type	Meaning	Description
SUBMIT	Submit	Submit
REJECT	Reject	Reject
ACCEPT	Accept	Accept
ADDITIONAL_INFO	Request for Additional Information	Request for Additional Information
REPLY	Respond to Request for Information	Respond to Request for Information

Lookup Type	Meaning	Description
WITHDRAW	Withdraw	Withdraw
SAVE	Save	Save
CLOSE	Close	Close

GRC_ISSUE_DOMAIN_TYPE Lookup Type

Lookup Code	Meaning	Description
RISK	Risk	Risk
PROCESS	Process	Process
CONTROL	Control	Control
PERSPECTIVE_ITEM	Perspective Item	Perspective Item

GRC_ISSUE_LIKELIHOOD Lookup Type

Lookup Code	Meaning	Description
LOW	Low	Low
MEDIUM	Medium	Medium
HIGH	High	High

GRC_ISSUE_PROGRESS Lookup Type

Lookup Code	Meaning	Description
DELAYED	Delayed	Delayed
ON_TARGET	On Target	On Target
COMPLETED	Completed	Completed

GRC_ISSUE_REASON Lookup Type

Lookup Code	Meaning	Description
NON_ISSUE	Non-Issue	Non-Issue
RESOLVED	Resolved	Resolved
REMEDIATION_COMPLETE	Remediation Complete	Remediation Complete
DUPLICATE	Duplicate	Duplicate
UNRESOLVED	Unresolved	Unresolved

GRC_ISSUE_REGIONAL_SEARCH_LIST Lookup Type

Lookup Code	Meaning	Description
REMED_PLANS	Remediation Plans	Remediation Plans
ISSUES	Issues	Issues

GRC_ISSUE_SEVERITY Lookup Type

Lookup Code	Meaning	Description
SIGNIFICANT_DEFICIENCY	Significant Deficiency	Significant Deficiency
DEFICIENCY	Deficiency	Deficiency
MINOR_GAP	Minor Gap	Minor Gap
DOCUMENTATION_ONLY	Documentation Only	Documentation Only

GRC_ISSUE_SOURCE Lookup Type

Lookup Code	Meaning	Description
INTERNAL	Internal	Internal - submitted from within GRC
EXTERNAL	External	External - submitted from outside of GRC

GRC_ISSUE_STATUS Lookup Type

Lookup Code	Meaning	Description
REMEDIATION	In Remediation	In Remediation
OPEN	Open	Open
HOLD	On Hold	On Hold
CLOSED	Closed	Closed

GRC_JOB_ROLE_TYPE Lookup Type

Lookup Code	Meaning	Description
247	Job Role	Job Role

GRC_LIKELIHOOD Lookup Type

Lookup Code	Meaning	Description
OCCUR	Occurrences	Occurrences

GRC_LIKELIHOOD_MODEL_TYPE Lookup Type

Lookup Code	Meaning	Description
QUAL	Qualitative	Qualitative Analysis
SQUAN	Semi-Quantitative	Semi-Quantitative Analysis

GRC_MATRIX_OBJ_TYPE Lookup Type

Lookup Code	Meaning	Description
GRC_RISK	Risk	GRC Risk
GRC_CONTROL	Control	GRC Control

GRC_MODEL_STATE Lookup Type

Lookup Code	Meaning	Description
APPROVED	Approved	Approved
INVALID	Invalid	Invalid

GRC_MODEL_STATUS Lookup Type

Lookup Code	Meaning	Description
INACTIVE	Inactive	Inactive
ACTIVE	Active	Active

GRC_MODEL_TYPE Lookup Type

Lookup Code	Meaning	Description
203	CONDITION	CONDITION
202	ACCESS	ACCESS
2	Transaction - Defined	Transaction - Defined
201	Transaction - Pattern	Transaction - Pattern

GRC_MYSURVEY_SEARCH_STATE Lookup Type

Lookup Code	Meaning	Description
OPEN	Open	Open
CLOSE	Closed	Closed

GRC_OBJECT_CLASS Lookup Type

Lookup Code	Meaning	Description
B	Base	Base Object Class
S	System Custom Object Type	System Custom Object Type Class
I	Inherited Class	Inherited Object Class
U	User Custom Object Type	User Custom Object Type Class

GRC_OBJECT_CONFIG_FEATURE Lookup Type

Lookup Code	Meaning	Description
1	Show	Show
3	Hide and Default	Hide and Default
2	Hide	Hide

GRC_PENDING_ACTIVITY_ACTION Lookup Type

Lookup Code	Meaning	Description
REVIEW	Review	Review
APPROVE	Approve	Approve
NEW	New	New
REVIEW_ASMT	Review Assessment	Review Assessment
APPROVE_ASMT	Approve Assessment	Approve Assessment
VALIDATE_ISSUE	Validate Issue	Validate Issue
INFO_REQUESTED	Information Requested	Information Requested
COMPLETE_RISK_ ANALYSIS	Complete Risk Analysis	Complete Risk Analysis
COMPLETE_RISK_ EVALUATION	Complete Risk Evaluation	Complete Risk Evaluation
VALIDATE_PROPOSED_ RISK	Validate Proposed Risk	Validate Proposed Risk
COMPLETE_ACTION_ ITEM	Complete Action Item	Complete Action Item
INVESTIGATE	Investigate	Investigate
COMPLETE_ASMT	Complete Assessment	Complete Assessment

GRC_PERSPECTIVE_ITEM Lookup Type

Lookup Code	Meaning	Description
RETIRE	Inactive	Open
NEW	New	New
ACTIVE	Active	Reported

Lookup Code	Meaning	Description
PROCESSING	Work in Progress	Work in Progress
REVIEW	In Review	In Review
APPROVE	Awaiting Approval	Awaiting Approval
RETIRE_REVIEW	In Review	In Review
RETIRE_APPROVE	Awaiting Approval	Awaiting Approval

GRC_PERSPECTIVE_TREE Lookup Type

Lookup Code	Meaning	Description
RETIRE	Inactive	Inactive
ACTIVE	Active	Active
REVIEW	In Review	In Review
APPROVE	Awaiting Approval	Awaiting Approval
RETIRE_REVIEW	In Review	In Review
NEW	New	New
RETIRE_APPROVE	Awaiting Approval	Awaiting Approval
PROCESSING	Work In Progress	Work In Progress

GRC_PERSP_REGIONAL_SEARCH_LIST Lookup Type

Lookup Code	Meaning	Description
PERSP_TREES	Perspective Hierarchies	Perspective Hierarchies
PERSP_ITEMS	Perspective Items	Perspective Items

GRC_PRINCIPAL_TYPE Lookup Type

Lookup Code	Meaning	Description
USER	User	User
ROLE	Role	Role

GRC_PROCESS Lookup Type

Lookup Code	Meaning	Description
RETIRE	Inactive	Inactive
RETIRE_REVIEW	In Review	In Review
NEW	New	New
RETIRE_APPROVE	Awaiting Approval	Awaiting Approval
APPROVE	Awaiting Approval	Awaiting Approval

Lookup Code	Meaning	Description
ACTIVE	Active	Active
PROCESSING	Work In Progress	Work In Progress
REVIEW	In Review	In Review

GRC_PROCESS_STATE Lookup Type

Lookup Code	Meaning	Description
APPROVE	Awaiting Approval	Awaiting Approval
REJECTED	Rejected	Rejected
ADDL_INFO_APPROVE	Request for Information In Approval	Request for Information In Approval
ADDL_INFO_REVIEW	Request for Information In Review	Request for Information In Review
EDIT	In Edit	In Edit
REVIEW	In Review	In Review
NEW	New	New
APPROVED	Approved	Approved

GRC_PROC_REGIONAL_SEARCH_LIST Lookup Type

Lookup Code	Meaning	Description
PROCESSES	Processes	Processes

GRC_PROPOSED_RISK Lookup Type

Lookup Code	Meaning	Description
REPORTED	Reported	Reported
NOTAPPLICABLE	Not Applicable	Not Applicable
ACTIVE	Active	Active
NEW	New	New

GRC_REMEDIATION_PLAN_STATUS Lookup Type

Lookup Code	Meaning	Description
OPEN	Open	Open
REMEDIATION	In Remediation	In Remediation
HOLD	On Hold	On Hold
COMPLETED	Completed	Completed
ACTIVE	Active	Active

Lookup Code	Meaning	Description
INACTIVE	Inactive	Inactive
CLOSED	Closed	Closed

GRC_REMED_PLAN Lookup Type

Lookup Code	Meaning	Description
ACTIVE	Active	Active
COMPLETE	Complete	Complete
APPROVE	Awaiting Approval	Awaiting Approval
REVIEW	In Review	In Review
PROCESSING	Work in Progress	Work in Progress
NEW	New	New

GRC_REMED_PLAN_ACTION Lookup Type

Lookup Code	Meaning	Description
REPLY	Respond to Request for Information	Respond to Request for Information
WITHDRAW	Withdraw	Withdraw
MARK_COMPLETE	Mark Complete	Mark Complete
ACCEPT	Accept	Accept
REJECT	Reject	Reject
ADDITIONAL_INFO	Request for Additional Information	Request for Additional Information
SUBMIT	Submit	Submit
SAVE	Save	Save

GRC_REMED_PLAN_PRIORITY Lookup Type

Lookup Code	Meaning	Description
LOW	Low	Low
MEDIUM	Medium	Medium
HIGH	High	High

GRC_REMED_PLAN_PROGRESS Lookup Type

Lookup Code	Meaning	Description
BLOCKED	Blocked	Blocked
DELAYED	Delayed	Delayed

Lookup Code	Meaning	Description
ON_TARGET	On Target	On Target
COMPLETED	Completed	Completed

GRC_REMED_TASK Lookup Type

Lookup Code	Meaning	Description
COMPLETED	Completed	Completed
ACTIVE	Active	Active

GRC_REMED_TASK_PRIORITY Lookup Type

Lookup Code	Meaning	Description
MEDIUM	Medium	Medium
HIGH	High	High
LOW	Low	Low

GRC_REMED_TASK_PROGRESS Lookup Type

Lookup Code	Meaning	Description
ON_TARGET	On Target	On Target
DELAYED	Delayed	Delayed
BLOCKED	Blocked	Blocked

GRC_RESPONSE_CATETGORY Lookup Type

Lookup Code	Meaning	Description
WARNING	Warning	Warning
SUCCESS	Success	Success
FAIL	Fail	Fail

GRC_RESPONSE_STATUS Lookup Type

Lookup Code	Meaning	Description
COMPLETE	Complete	Complete
PARTIALLY_COMPLETE	Partially Complete	Partially Complete
NOT_STARTED	Not Started	Not Started

GRC_REVIEW_ACTION Lookup Type

Lookup Code	Meaning	Description
RETURN	Return for information	Return for more information
REJECT	Reject	Rejected
REVIEW	Review complete	Review complete

GRC_RISK Lookup Type

Lookup Code	Meaning	Description
APPROVE	Awaiting Approval	Awaiting Approval
RETIRE_APPROVE	Awaiting Approval	Awaiting Approval
ACTIVE	Active	Active
RETIRE	Inactive	Inactive
REVIEW	In Review	In Review
RETIRE_REVIEW	In Review	In Review
NONE	None	None
NEW	New	New
PROCESSING	Work In Progress	Work In Progress

GRC_RISK_ANALYSIS Lookup Type

Lookup Code	Meaning	Description
PROCESSING	Work in Progress	Work in Progress
COMPLETE	Complete	Complete

GRC_RISK_ANALYSIS_FORMULA_TYPE Lookup Type

Lookup Code	Meaning	Description
P	Product (Formula: Risk Level = Likelihood x Impact)	Product (Formula: Risk Level = Likelihood x Impact)
W	Weighted Product (Risk Lvl = Exp((Impact*Weight Factor),X) * Exp(Likelihood,Y))	Weighted Product (Formula: Risk Level = Exp((Impact * Weighting Factor), X) * Exp(Likelihood, Y))

GRC_RISK_ANALYSIS_MODEL Lookup Type

Lookup Code	Meaning	Description
APPROVE	Awaiting Approval	Awaiting Approval
REVIEW	In Review	In Review
RETIRE	Inactive	Inactive

Lookup Code	Meaning	Description
ACTIVE	Active	Active
NEW	New	New
PROCESSING	Work In Progress	Work In Progress

GRC_RISK_ANALYSIS_MODEL_TYPE Lookup Type

Lookup Code	Meaning	Description
QUAL	Qualitative	Qualitative Analysis Model
QUAN	Quantitative	Quantitative Analysis Model

GRC_RISK_ANALYSIS_TYPE Lookup Type

Lookup Code	Meaning	Description
SQUAL	Semi-Qualitative	Semi-Qualitative Analysis
QUAL	Qualitative	Qualitative Analysis
SQUAN	Semi-Quantitative	Semi-Quantitative Analysis
QUAN	Quantitative	Quantitative Analysis

GRC_RISK_CONTEXT_MODEL Lookup Type

Lookup Code	Meaning	Description
RETIRE	Inactive	Inactive
ACTIVE	Active	Active
NEW	New	New

GRC_RISK_EVALUATION Lookup Type

Lookup Code	Meaning	Description
PROCESSING	Work in Progress	Work in Progress
COMPLETE	Complete	Complete

GRC_RISK_HEATMAP_TYPE Lookup Type

Lookup Code	Meaning	Description
INHERENT	Inherent	Inherent
RESIDUAL	Residual	Residual
TARGET	Target	Target

GRC_RISK_OVERVIEW_VIEWBY Lookup Type

Lookup Code	Meaning	Description
SIGNIFICANCE	Significance	Significance
TOLERANCE	Tolerance	Tolerance

GRC_RISK_PROPSL_PTNTL_OUTCOME Lookup Type

Lookup Code	Meaning	Description
THREAT	Threat	Threat
OPPORTUNITY	Opportunity	Opportunity

GRC_RISK_REGIONAL_SEARCH_LIST Lookup Type

Lookup Code	Meaning	Description
EVENT	Event	Event
RISK	Risk	Risk
CONSEQUENCE	Consequence	Consequence

GRC_RISK_SIG_MODEL Lookup Type

Lookup Code	Meaning	Description
NEW	New	New
ACTIVE	Active	Active
RETIRE	Inactive	Inactive

GRC_RISK_STATE Lookup Type

Lookup Code	Meaning	Description
ADDL_INFO_APPROVE	Request for Information In Approval	Request for Information In Approval
REVIEW	In Review	In Review
APPROVE	Awaiting Approval	Awaiting Approval
APPROVED	Approved	Approved
REJECTED	Rejected	Rejected
EDIT	In Edit	In Edit
ADDL_INFO_REVIEW	Request for Information In Review	Request for Information In Review
NEW	New	New

GRC_RISK_TOLERANCE Lookup Type

Lookup Code	Meaning	Description
1	Accepted	Accepted
3	Treat	Treat
2	Monitor	Monitor

GRC_ROLE_STATUS Lookup Type

Lookup Code	Meaning	Description
52	Inactive	Inactive
51	Active	Active

GRC_ROLE_TYPE Lookup Type

Lookup Code	Meaning	Description
247	Job Role	Job Role
246	Duty Role	Duty Role
245	Data Role	Data Role

GRC_SECURITY_CONDITION Lookup Type

Lookup Code	Meaning	Description
EQUALS	Equals	Equals
NOT_EQUALS	Not Equals	Not Equals
INCLUDES_CHILDREN	Includes Children	Includes Children

GRC_SECURITY_OBJECT Lookup Type

Lookup Code	Meaning	Description
DATA_ATTRIBUTE	Data Attributes	Data Attributes
PERSPECTIVE	Perspectives	Perspectives

GRC_SEC_DATA_ATTRIBUTE Lookup Type

Lookup Code	Meaning	Description
Module	Module	Module
DataRole	DataRole	DataRole
State	State	State
StateAction	StateAction	StateAction

GRC_SEC_DATA_ATTRIBUTE_ACTION Lookup Type

Lookup Code	Meaning	Description
Delete	Delete	Delete
View	View	View
Edit	Edit	Edit

GRC_SURVEY Lookup Type

Lookup Code	Meaning	Description
NONE	None	None
RETIRE_REVIEW	In Review	In Review
RETIRE_APPROVE	Awaiting Approval	Awaiting Approval
REVIEW	In Review	In Review
APPROVE	Awaiting Approval	Awaiting Approval
PROCESSING	Work In Progress	Work In Progress
RETIRE	Inactive	Inactive
NEW	New	New
ACTIVE	Active	Active

GRC_SURVEY_PARTICIPANT_STATUS Lookup Type

Lookup Code	Meaning	Description
OPEN	Not Started	Not Started
COMPLETED	Completed	Completed
PARTIALLY_COMPLETED	Partially Complete	Partially Complete
STARTED	Started	Started
NEW	Not Started	Not Started

GRC_SURVEY_QUESTION Lookup Type

Lookup Code	Meaning	Description
ACTIVE	Active	Active
RETIRE	Inactive	Inactive
NEW	New	New
PROCESSING	Work in Progress	Work in Progress

GRC_SURVEY_QUESTION_DSP_CHOICE Lookup Type

Lookup Code	Meaning	Description
ROW	In a row	In a row
2COL	In 2 columns	In 2 columns
COL	In a column	In a column

GRC_SURVEY_QUESTION_FMT_TYPE Lookup Type

Lookup Code	Meaning	Description
SINGLE_LIST	Single Response Drop Down List	Single Response Drop Down List
MULTI_LIST	Multiple Choice List Box	Multiple Choice List Box
NUMERIC	Numeric Allocation	Numeric Allocation
RADIO	Single Response	Single Response
RADIO_OTHER	Single Response with Other	Single Response, with Other (Please Specify)
CHECK	Check all that apply	Check all that apply
CHECK_OTHER	Check all that apply with Other	Check all that apply, with Other (Please Specify)
OPEN_TEXT	Open Text	Open Text
RATING	Rating on Scale	Rating on Scale

GRC_SURVEY_QUESTION_TYPE Lookup Type

Lookup Code	Meaning	Description
GENERAL	General	General
CERT_302	302 Certification	302 Certification
FIN_COMP	Financial Compliance	Financial Compliance

GRC_SURVEY_START_STATUS Lookup Type

Lookup Code	Meaning	Description
SCHEDULE	Scheduled	Scheduled
OPEN	Open	Open
NEW	New	New
CLOSE	Closed	Closed

GRC_SURVEY_STATE Lookup Type

Lookup Code	Meaning	Description
NEW	New	New
OPEN	Open	Open
CLOSED	Closed	Closed

GRC_SURVEY_SURVEY_TYPE Lookup Type

Lookup Code	Meaning	Description
GENERAL	General	GENERAL
CERT_302	302 Certification	302 Certification
FIN_COMP	Financial Compliance	Financial Compliance

GRC_SURVEY_TEMPLATE Lookup Type

Lookup Code	Meaning	Description
RETIRE_APPROVE	Awaiting Approval	Awaiting Approval
PROCESSING	Work In Progress	Work In Progress
RETIRE_REVIEW	In Review	In Review
NEW	New	New
ACTIVE	Active	Active
RETIRE	Inactive	Inactive
APPROVE	Awaiting Approval	Awaiting Approval
REVIEW	In Review	In Review

GRC_TASK_TYPE Lookup Type

Lookup Code	Meaning	Description
GRC_ASMT_RESULT	Complete Assessment	Complete Assessment
GRC_PR	Proposed Risk	Proposed Risk
GRC_IM	Issue Management Overview	Issue Management Overview
GRC_ISSUES_DRAFT	Issue New	Issue New
GRC_SURVEY	Survey	Survey
GRC_SURVEY_ COMPLETE	Complete Survey	Complete Survey
GRC_ASMT_SURVEY_ COMPLETE	Complete Assessment Survey	Complete Assessment Survey
GRC_RISK_ANALYSIS_ COMPLETE	Complete Risk Analysis	Complete Risk Analysis
GRC_RISK_ANALYSIS_FYI	Completed Risk Analysis	Completed Risk Analysis

Lookup Code	Meaning	Description
GRC_PERSP	Perspective Management Overview	Perspective Management Overview
GRC_CTRL_TPA_DRAFT	New Test Plan Activity	New Test Plan Activity
GRC_CTRL_TP_DRAFT	Control Test Plan Draft	Control Test Plan Draft
GRC_CTRL_TPA_ACTIVE	Active Test Plan Activity	Active Test Plan Activity
GRC_CM	Control Management Overview	Control Management Overview
GRC_PRISK_REJECT_FYI	Rejected Proposed Risk	Rejected Proposed Risk
LINE_MANAGER_ APPROVAL	Line Manager Approval	Line Manager Approval
RISK_MANAGER_ ASSESSMENT	Risk Manager Assessment	Risk Manager Assessment
GRC_PRISK_DRAFT	New Proposed Risk	New Proposed Risk
GRC_RM	Risk Management Overview	Risk Management Overview
GRC_RISK_ACTIVE	Risk Active	Risk Active
GRC_RISK_DRAFT	Risk Draft	Risk Draft
GRC_TREATMENTPLAN_ DRAFT	Treatment Plan Draft	Treatment Plan Draft
GRC_TREATMENTPLAN_ ACTIVE	Treatment Plan Active	Treatment Plan Active
GRC_TREATMENTACTIVI TY_DRAFT	Treatment Activity Draft	Treatment Activity Draft
GRC_TREATMENTACTIVI TY_ACTIVE	Treatment Activity Active	Treatment Activity Active
GRC_CONSEQUENCE_ ACTIVE	Consequence Active	Consequence Active
GRC_CONSEQUENCE_ DRAFT	Consequence Draft	Consequence Draft
GRC_EVENT_DRAFT	Event Draft	Event Draft
GRC_EVENT_ACTIVE	Event Active	Event Active
GRC_PRISK_FYI	Active Proposed Risk Alert	Active Proposed Risk Alert
GRC_RISK_EVALUATION_ COMPLETE	Complete Risk Evaluation	Complete Risk Evaluation
GRC_RISK_EVALUATION_ FYI	Completed Risk Evaluation	Completed Risk Evaluation
GRC_AM	GRC Tools Management Overview	GRC Tools Management Overview
GRC_HOME	My GRC Overview	My GRC Overview
GRC_DRAFT	New	New
GRC_REVIEW	To Be Reviewed	To Be Reviewed
GRC_APPROVE	Requires Approval	Requires Approval

Lookup Code	Meaning	Description
GRC_UPSTREAM_FYI	Related Component Modified	Related Component Modified
GRC_COMPONENT	Component Management Overview	Component Management Overview
GRC_NOTIFY_REVIEWED	Reviewed	Reviewed
GRC_NOTIFY_APPROVED	Approved	Approved
GRC_NOTIFY_REJECTED	Rejected	Rejected
GRC_INFO_REQUESTED	Information Requested	Information Requested

GRC_TEMP_CURRENCY_CODE Lookup Type

Lookup Code	Meaning	Description
USD	US dollar	US dollar
EUR	EU euro	EU euro
CAD	Canadian dollar	Canadian dollar
GBP	British pound	British pound
JPY	Japanese yen	Japanese yen
MXN	Mexican peso	Mexican peso

GRC_TEST_INSTRUCTION_TYPE Lookup Type

Lookup Code	Meaning	Description
MANUAL	manual test instruction	manual test instruction

GRC_TEST_PLAN_FREQUENCY Lookup Type

Lookup Code	Meaning	Description
MONTHLY	Monthly	Monthly
WEEKLY	Weekly	Weekly
DAILY	Daily	Daily
YEARLY	Yearly	Yearly

GRC_TREATMENT_LEVEL Lookup Type

Lookup Code	Meaning	Description
PRIMARY	Primary	Primary
SUBORDINATE	Subordinate	Subordinate

GRC_TREATMENT_STRATIFICATION Lookup Type

Lookup Code	Meaning	Description
KEY	Key	Key
OTHER	Other	Other
MONITORING	Monitoring	Monitoring
COMPENSATING	Compensating	Compensating
REDUNDANT	Redundant	Redundant
MITIGATING	Mitigating	Mitigating

GRC_TREATMENT_TYPE Lookup Type

Lookup Code	Meaning	Description
SHARED	Shared	Shared
REDUCTION	Reduction	Reduction
AVOID	Avoid	Avoid
RETAINED	Retained	Retained

GRC_TRUE_FALSE Lookup Type

Lookup Code	Meaning	Description
FALSE	False	False
True	True	true

GRC_UDA_CONTROL_TYPE Lookup Type

Lookup Code	Meaning	Description
05	Multiple Line Text Box	Multiple Line Text Box
02	Date Picker	Date Picker
03	Check Box	Check Box
04	Drop-down	Drop-down
01	Text Box	Text Box

GRC_UDA_DATA_TYPE Lookup Type

Lookup Code	Meaning	Description
SN	String NonTranslatable	String NonTranslatable
ST	String Translatable	String Translatable
D	Date	Date
N	Number	Number
L	Link	Link

GRC_URL_TYPE Lookup Type

Lookup Code	Meaning	Description
BIP_REPORT	BIP Report	BIP Report
URL_LINK	URL Link	URL Link

GRC_USER_STATUS Lookup Type

Lookup Code	Meaning	Description
40	Active	Active
41	Inactive	Inactive
42	Locked	Locked

GRC_VACATION_ACTION Lookup Type

Lookup Code	Meaning	Description
D	Delegate	Delegate
N	No Action	No Action
R	Reassign	Reassign

GRC_VALUESET_LEVEL_5 Lookup Type

Lookup Code	Meaning	Description
5	High	High
3	Medium	Medium
2	Medium Low	Medium Low
1	Low	Low
4	Medium High	Medium High

GRC_YES_NO Lookup Table

Lookup Code	Meaning	Description
N	No	No
Y	Yes	Yes

ISSUE_OVERVIEW_SELECTION Lookup Type

Lookup Code	Meaning	Description
STATUS	Status	Status
LIKELIHOOD	Likelihood	Likelihood

ISSUE_SOURCE Lookup Type

Lookup Code	Meaning	Description
INTERNAL	Internal	Internal
EXTERNAL	External	External

JOB_STATUS Lookup Type

Lookup Code	Meaning	Description
166	Cancel Requested	Cancel Requested
167	Paused	Paused
35	In Progress	In Progress
33	Canceled	Canceled
32	Errored	Errored
31	Completed	Completed
30	Started	Started
165	Not Started	Not Started
168	Pause Requested	Pause Requested
169	Queued	Queued

JOB_STATUS_MESSAGE Lookup Type

Lookup Code	Meaning	Description
Job completed	Job completed	Job completed
Job started	Job started	Job started
Job canceled	Job canceled	Job canceled
Job queued	Job queued	Job queued
NOT STARTED	NOT STARTED	NOT STARTED

JOB_TYPE Lookup Type

Lookup Code	Meaning	Description
TCGETL	TCGETL	TCGETL
PUSHETL	PUSHETL	PUSHETL

Lookup Code	Meaning	Description
WORKLIST_SYNC_JOB	Worklist Synchronizer Job	Worklist Synchronizer Job
GRC_OBJECT_WORKLIST_SYNC_JOB	GRC Object Worklists Synchronizer Job	GRC Object Worklists Synchronizer Job
INITIATE_ASSESSMENT	Initiate Assessment Job	Initiate Assessment Job
IMPORT_CUSTOM_BO_JOB	Import Custom BO	Import Custom BO
MASS_ASSIGNMENT	Mass Assignment	Mass Assignment
GRCCMODEL_ANALYSIS	GRCC Model Analysis	GRCC Model Analysis
EXPORT	Export	Export
PASSWORD_EXPIRATION_MESSAGE	Password Expiration Message	Password Expiration Message
ARCHIVE	Purge Conflict Run	Purge Conflict Run
SIMULATION_STATISTICS	Simulation Statistics	Simulation Statistics
MESSAGE_JOB	Notification	Notification
REPORT	Report	Report
USER_PROVISIONING	User Provisioning	User Provisioning
IMPORT	Import Data File	Import Data File
DATA_ANALYTICS	Data Analytics	Data Analytics
MIGRATION	Migration	Migration
GRCM_EXPORT	Generate Import Template	Generate Import Template
ETL	Datasource Synchronization	Datasource Synchronization
SIMULATION	Simulation	Simulation
CONTROL_ANALYSIS	Control Analysis	Control Analysis
SIMULATION_PROVISIONING	Simulation Provisioning	Simulation Provisioning

MODIFIER_TYPE_USERS Lookup Type

Lookup Code	Meaning	Description
USERS	Users	Users

NUMBER_FORMAT Lookup Type

Lookup Code	Meaning	Description
#,##0.###	-1,234.567	-1,234.567
#,##0.###;#,##0.###-	1,234.567 / 1,234.567-	1,234.567 / 1,234.567-
#,##0.###;(#,##0.###)[.,]	1.234,567 / (1.234,567)	1.234,567 / (1.234,567)
#,##0.###[',]	-1'234,567	-1'234,567
#,##0.##[\u00A0,]	-1 234,56	-1 234,56

Lookup Code	Meaning	Description
#,##0.###[.,]	-1.234,567	-1.234,567
#,##0.###[\u00A0,]	-1 234,567	-1 234,567
#,##0.##[.,]	-1.234,56	-1.234,56
#,##0.###['.]	-1'234.567	-1'234.567

ONTCLASS_TYPE Lookup Type

Lookup Code	Meaning	Description
137	HR	HR
140	Procurement	Procurement
139	Supply Chain	Supply Chain
138	Financial	Financial

TEMP_LOCATION Lookup Type

Lookup Code	Meaning	Description
PTN	Pleasanton	Pleasanton, CA, USA
RWS	Redwood Shores	Redwood Shores, CA, USA
CSP	Colorado Springs	Colorado Springs, CO, USA

TIME_FORMAT Lookup Type

Lookup Code	Meaning	Description
HH.mm	(00.12)	(00.12)
HH.mm.ss	(00.12.34)	(00.12.34)
HH:mm	(00:12)	(00:12)
HH:mm:ss	(00:12:34)	(00:12:34)
a hh.mm	(AM 12.34)	(AM 12.34)
a hh.mm.ss	(AM 12.34.56)	(AM 12.34.56)
a hh:mm	(AM 12:34)	(AM 12:34)
a hh:mm:ss	(AM 12:34:56)	(AM 12:34:56)
hh.mm a	(12.34 AM)	(12.34 AM)
hh.mm.ss a	(12.34.56 AM)	(12.34.56 AM)
hh:mm a	(12:34 AM)	(12:34 AM)
hh:mm:ss a	(12:34:56 AM)	(12:34:56 AM)
H:mm:ss	(0:12:34)	(0:12:34)
H:mm	(0:12)	(0:12)
H.mm	(0.12)	(0.12)
H.mm.ss	(0.12.34)	(0.12.34)

USER_PROV Lookup Type

Lookup Code	Meaning	Description
55	Rejected	Rejected
56	Prevented	Prevented
53	Pending	Pending
54	Approved	Approved

USER_PROV_FOR_APPROV Lookup Type

Lookup Code	Meaning	Description
54	Approve	Approve
53	Pending	Pending
55	Reject	Reject

USER_PROV_STATUS Lookup Type

Lookup Code	Meaning	Description
55	Rejected	Rejected
54	Approved	Approved
53	Pending	Pending