Oracle® Governance, Risk and Compliance Controls

User Guide

Release 8.5.1

December 2009

ORACLE

Oracle Governance, Risk and Compliance Controls User Guide

Primary Author: David Christie

Contents

1

Introduction

Governance, Risk and Compliance Controls (GRCC) provides a platform in which two applications run. They can impose controls by default on instances of Oracle E-Business Suite and PeopleSoft Enterprise, and may be configured to work with other business-management applications as well.

- Transaction Controls Governor (TCG) enables users to define "models," each of which specifies circumstances under which individual transactions would pose an unacceptable risk to a company.
- Application Access Controls Governor (AACG) regulates access to duties assigned in business-management applications. It implements "access policies," which identify duties that are considered to conflict with one another because, in combination, they would enable individual users to complete transactions that may expose a company to risk.

In earlier versions (8.0 through 8.2.1), the platform contained only AACG, and the product was known as Application Access Controls Governor. Version 8.5.0 added TCG to the platform, and as a result the product as a whole is now called Governance, Risk and Compliance Controls.

Although TCG and AACG have distinct feature sets, they also share functionality provided by the GRCC platform. These features include tools to connect GRCC to Oracle, PeopleSoft, and other business-management-application datasources (instances), and to refresh "snapshots" of data gathered from those applications; to create GRCC users and user roles; and to set GRCC parameters, connect with your email server (for the purpose of sending notifications to GRCC users), and integrate GRCC with other applications. Moreover, the GRCC platform can display information in any of eleven languages.

These shared features are the subject of this *Governance, Risk and Compliance Controls User Guide*. For information on the creation of access policies and analysis of the conflicts they generate, see the *Application Access Controls Governor User Guide*. For information on the creation of models and the review of risky transactions they identify, see the *Transaction Controls Governor User Guide*.

GRCC and Language

Governance, Risk and Compliance Controls can display information in any of eleven languages: US English, standard (simplified) Chinese, traditional Chinese, Danish, French, German, Italian, Japanese, Korean, Brazilian Portuguese, or Spanish. An administrator uses the Application Configuration panel to make a selection of these languages available to users (see page 3-7).

Each individual user may select one of the available languages while logging on (see page 1-3), while configuring a user profile (see page 2-9), or both. For a given user, GRCC "selects" a language in the following order of preference:

- The language specified during logon.
- If none is selected then, the language specified in the user profile.
- If no language is chosen in either place, the language specified in the user's web browser.
- If the web browser language does not match one available in the AACG instance, US English.

GRCC may connect to any number of datasources (instances of business-management applications; see page 3-1). 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, GRCC follows these rules:

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

  Thus, for example, if a user logged on to GRCC 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, GRCC 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 to GRCC in French, and the instance were connected to a datasource that defined AACG access policies in both French and German, it would display the French policies (and the conflicts generated by them), but omit the German policies (and their conflicts).

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

Starting Governance, Risk and Compliance Controls

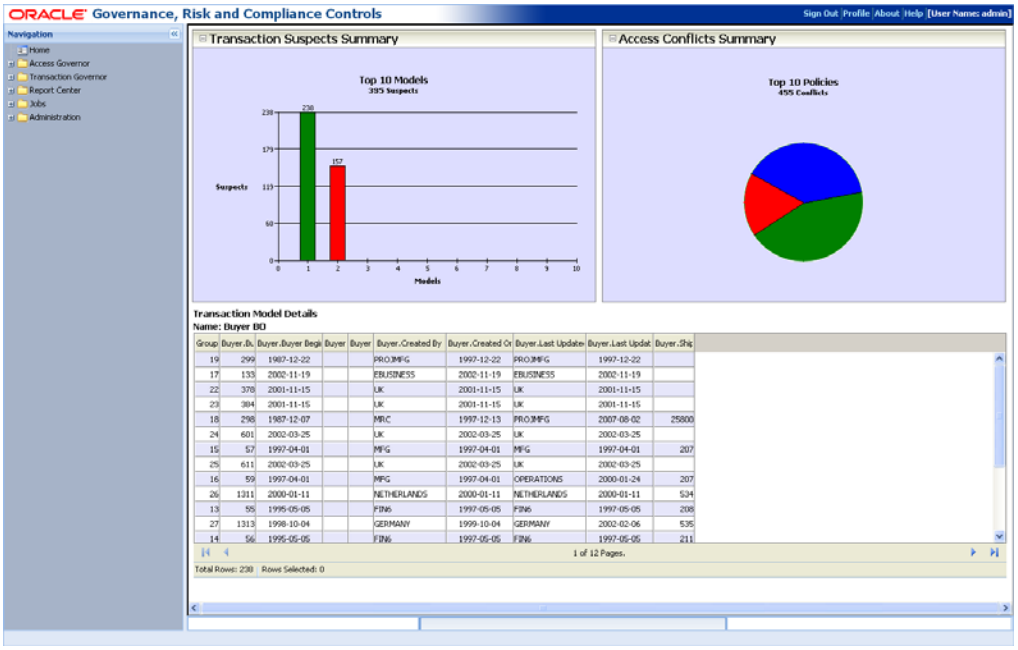
To start the Governance, Risk and Compliance Controls platform:

1. Open a web browser.
2. In the Address field, type the URL for your instance of Governance, Risk and Compliance Controls, and press the Enter key.
3. A Login dialog box appears. Type your user name and password in the appropriate fields, optionally, select a language in which to work in the Language Preference list box, and click on the Login button.

   You can leave the Language Preference field blank. If so, GRCC selects (in order of preference) the language specified in your user profile (see page 2-9), the language of your web browser, or US English.

Navigation

The left column of the GRCC user interface is a Navigation panel. To its right, a frame initially displays a Home page (shown below), but then presents items you select in the Navigation panel.



Using the Navigation Panel

Of the top-level nodes in the Navigation panel, Home, Administration, and Jobs present links to features that are the focus of this *User Guide*. See the *Transaction Controls Governor User Guide* for information on features available from the Transaction Governor node, or the *Application Access Controls Governor User Guide* for features available from the Access Governor and Report Center nodes.

When you select a high-level link, it opens a list of subordinate links. Some of these display a box containing a symbol that toggles between a plus sign and a minus sign. These entries provide a path to lower-level entries, but do not themselves open pages in which you can work. Click on a plus sign to reveal lower-level entries; click on a minus sign to hide the lower-level entries from view. When you reach an entry with no plus or minus sign, click on the entry to open pages in the frame to the right.

To expand the Navigation panel, position the mouse cursor over its right border, hold down the left mouse button, and drag the border to the right. Having done so, you can drag the border to the left, causing the panel to contract up to its original size. To close the Navigation panel entirely (and so expand the frame in which you will be working), click on the button with the << symbol, located at the top right of the Navigation panel. The button then changes to display a >> symbol; click on it to reopen the Navigation panel.

Viewing the Home Page

When you log on to GRCC, a Home page is displayed; if you navigate away from it, you can return to it by selecting the Home node in the Navigation panel. The Home page contains two graphs:

- A bar graph depicts the ten TCG models that have identified the greatest numbers of risky transactions. Each bar represents a model, its height proportional to the number of transactions identified by that model.
- A pie graph depicts the ten AACG access policies that have generated the greatest numbers of conflicts. Each “pie slice” represents a policy, its area proportional to the number of conflicts generated by that policy.

Click on a bar in the TCG graph or a pie slice in the AACG graph. A grid below the graphs displays information about the transactions or conflicts returned by the selected model or policy.

Creating Views

In lists — such as the Users pane of the User Administration page — you can limit the display of entries to those that satisfy filtering criteria, and you can sort the entries. You can also remove columns from display, or restore them; rearrange the order in which columns appear; and resize them. You can then save your selections as a “view,” and then either select your view for display or cause it to be displayed by default.

Filtering Data

To filter the values displayed in a list:

1. Determine where to enter filtering criteria. In some lists, you do so in text boxes that appear directly below column headings. Some lists omit these text boxes; in these, you enter filtering criteria in the first row of the list.
2. In any combination of columns in the view row or text boxes, enter (or select) values appropriate to the columns.
3. Click on the View button in the tool bar above the list. The list then contains only entries that match the values you've entered.

For columns that accept values, the percent sign (%) serves as a wild-card character. If it is placed after a string of text or numbers, the view returns all values that begin with the string. If it is placed before a string, the view returns all values that end with the string. If it is placed both before and after a string, the view returns all values in which the string appears at any position. If you omit the wild-card character, the view returns only a value that matches the string exactly.

Sorting Data

To set a sort order for items in a list, click in the heading for one of its columns. Entries in that column are then arranged in alphanumeric order (and entries in other columns are, of course, rearranged so that rows remain intact). Click in the column heading a second time to arrange entries in reverse alphanumeric order.

Removing and Restoring Columns

To remove columns from display, or to restore them:

1. Right click in the header row of the list from which you wish to remove columns, or to which you wish to restore them.
2. In some cases, a menu appears. If so, position the mouse cursor over its Columns option, and a list of available columns appears. In other cases, the parent menu does not appear, and the list of available columns opens directly.
3. To remove a column from view, click on its check box so that its check mark disappears. To restore a column to view, click on its check box so that its check mark reappears.
4. Left click anywhere outside of the menu and list of columns to close them.

Rearranging Columns

To rearrange the order in which columns appear:

1. Position the mouse cursor over a column you want to move, and hold down the left mouse button.
2. A "shadow" instance of the column heading appears. Continue to hold down the left mouse button, and drag that instance to the right or left.

3. Blue arrows appear — one above and one below the header row — to show where the column will be inserted. When they appear at the position you want, release the left mouse button.

Resizing Columns

To alter the width of columns in lists:

1. In the row that displays column titles, position the mouse cursor over the faint bar that separates one column from another.
2. The cursor changes to look like a pair of parallel vertical lines, each with an arrow extending horizontally from it. When that happens, hold down the left mouse button and drag the column border to the left or right.

Saving or Deleting a View

In most cases, there is a Manage View button. If so, you can save the view you define. To do so:

1. Define the view: In a list, set filtering criteria and sort order for data entries, and select, arrange, and resize columns as you wish.
2. Click on the Manage View button. A Manage View dialog opens.
3. Enter values and click on the Save button:
    - Create a new name in the “Type new view name” field. The new view criteria are then saved under the new name.
    - Use the “Select view name to override” list box to select an existing view. Its name is retained, but the new criteria replace earlier values. If you choose a value in the “Select view name to override” list box, the “Type a new view name” field becomes inactive, and you cannot enter a value in it.
    - If you want this view to appear each time you open the page in which you are working, select the Set as Default check box. There can be only one default view, so when you select this check box for a view, it overrides any prior selections involving other views.

You can also delete a saved view. To do so, open the Manage View dialog, select the view in the “Select view name to override” field, and click on the Delete button.

Displaying a View

To cause a list to display entries selected by a saved view:

1. Click on the downward-pointing triangle at the right of the View button.
2. A list of saved views appears. Click on the one you want to use.

Finally, to override a selected view (whether saved or defined ad hoc), click on the Clear View button. This causes all entries to disappear from the list; to restore content, either select (or define) another view, or click on the View button to display all possible entries.

2

User and Role Administration

Using tools available in the Administration area, you can create roles, each of which grants access to a set of features in Governance, Risk and Compliance Controls. You can then create users and assign roles to them. Each user can have any number of roles.

Viewing Roles

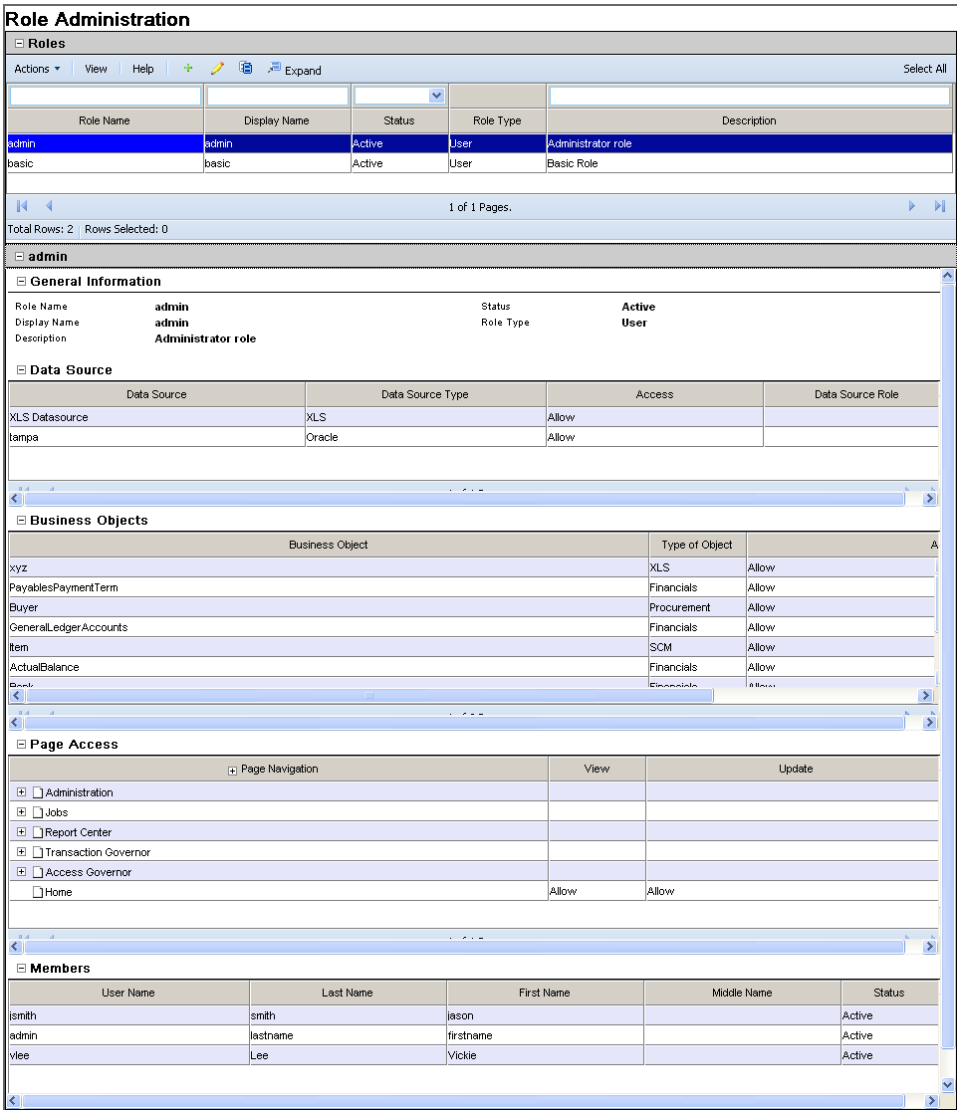
To view or work with roles, open a Role Administration page — select the Role Administration option in the Administration node of the Navigation panel.

The Role Administration page (shown at the top of the next page) provides information, in read-only format, about GRCC roles. Its upper pane, labeled “Roles,” displays a list of existing roles, together with summary information about each — the name and display name of the role, its status (active or inactive), and a description. The summary information also includes a type value — user (an individual role) or group (a set of two or more roles that confers all access defined by the constituent roles, any of which may itself be a user role or group role).

In the Roles pane, select (click on) the row for a role whose information you wish to review. A lower pane, labeled with the name of the selected role, displays detailed information about it. This pane is divided into a minimum of five parts:

- General Information displays the role name and other identifying information (entered in the General Information pane of the Create Role page as the role was created or edited; see page 2-3.)
- Datasource lists instances of business-management applications that have been configured (in the Data Administration page) to communicate with GRCC. For each, the value in an Access column — *Allow* or *Deny* — indicates whether the datasource may be incorporated into TCG models. (This setting applies specifically to TCG. For AACG, when a datasource is configured in the Data Administration page, that source is available for use in access policies and entitlements no matter how roles are configured.)

  The listing for each datasource includes a Type value — for example, *Oracle* if the datasource supports an Oracle EBS instance. If you have created “adapters” (software objects that enable other business-management applications to supply data to TCG), type values for these applications may also appear.



- Business Objects lists business objects available in the selected datasources — a "business object" being a set of one or more database tables that hold information pertinent to transactions subject to control by TCG models. For each business object, a value in an Access column — *Allow* or *Deny* — indicates whether the role has access to the object.
- Page Access displays a grid that expands to show all pages available in GRCC. (Entries in the grid mimic the hierarchy of the Navigation panel; click on the ± toggles to expand or contract levels in the hierarchy.) The grid also shows the access granted by the role to each page: for each, View and Update privileges are labeled either *Allow* or *Deny*. (These settings apply TCG, AACG, and GRCC functionality common to the two applications.)
- Members lists GRCC users who have been assigned the role, together with summary information about them.

If you have selected a group role, a sixth section appears: Roles in Group displays a list of the roles that have been incorporated into the group role.

Creating a User Role

If you intend to select a set of datasources, business objects, and page-access properties, so that they might be assigned to users, create a user role:

1. In the Role Administration page, click on Actions > Create New. Or click on the Create New icon — a green plus sign. A Create Role page opens.
2. Enter values in the General Information pane of the Create Role 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 Role Name field, enter a name for the role that is used internally by the system.
   - In the Display Name field, enter a name that suggests the role's purpose to GRCC users.
   - In the Description field, briefly explain the purpose of the role.
   - In the Status field, select Active or Inactive.
   - In the Role Type field, select User.
3. A Datasource pane lists instances of business-management applications that have been configured as datasources in the Data Administration page. Select any number of them; users assigned the role can incorporate the selected datasources into TCG models. For each, click on the cell in the Access column, and select the value *Allow*.

   Your datasource selections have no bearing on AACG. All datasources configured in the Data Administration page are available for use in access policies and entitlements no matter how roles are configured.

   Here and in the remaining panes (Business Objects and Page Access), you can select multiple rows and change the setting for all at once. To select a row, 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 rows. Or, to choose all rows, click Actions > Select All. When you finish selecting rows, click the Set All Selected button (or Actions > Set All Selected). A Set All Selected dialog opens; choose Deny or Allow in its list box, and click the OK button.
4. A Business Objects pane lists business objects available in the selected datasources (a "business object," once again, being a set of one or more database tables that hold information pertinent to transactions subject to control by TCG models). Select any number of them to enable users assigned the role to incorporate them in TCG models. For each, click on the cell in the Access column, and select the value *Allow*.
5. A Page Access pane displays a grid that expands to show all pages available in GRCC. (Entries in the grid mimic the hierarchy of the Navigation panel; click on the ± toggles to expand or contract levels in the hierarchy.) Select any number of pages to make them available to users assigned the role. For each, click in the View cell to provide read-only rights, or the View and Update columns to provide write access; select the value *Allow*.

Although you define access to pages, you need not define access to navigation nodes hierarchically above pages. For example, to grant access to any of the AACG Definition, Entitlements, Global Conditions, or Global Path Conditions pages, you need not assign rights to the Policy and Access Governor nodes above them.

Generally accepted segregation-of-duties practice holds that a user who creates policies should not also be able to review the conflicts they generate. So roles you create for User Provisioning typically should not also permit users to create policies. By default, GRCC provides an "admin" role that provides access to all functionality; the purpose of this role is to permit initial implementation of GRCC features. Before GRCC is deployed to a production environment, edit the admin role to conform to the generally accepted practice.

6. Save the role. Click on the Save button to save the role and reopen it in an Edit Role page. Or click a Save and Close button to save the role and return to the Role Administration page. (Alternatively, click a Cancel button to return to the Role Administration page without saving the role values you've configured.)

Although the Role Administration page displays the members (users) who have been assigned the role, you cannot select members directly in the Create Role page. You can modify membership only indirectly, by assigning the role to users in the User Administration page.

Creating a Group Role

If you intend to select a set of existing roles to be combined to form a more expansive role, create a group role:

1. In the Role Administration page, click on Actions > Create New. Or click on the Create New icon — a green plus sign. A Create Role page opens.
2. Enter values in the General Information pane of the Create Role 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 Role Name field, enter a name for the role that is used internally by the system.
   - In the Display Name field, enter a name that suggests the role's purpose to GRCC users.
   - In the Description field, briefly explain the purpose of the role.
   - In the Status field, select Active or Inactive.
   - In the Role Type field, select Group.

   The Create Role page refreshes, adding a Roles in Group pane immediately beneath the General Information pane.
3. Assign roles to the group role. You can assign existing user or group roles to the group role you are creating.
   - The Roles in Group pane of the Create Role page contains two boxes, one labeled *Available Roles* and the other *Selected Roles*. The Available Roles box displays entries for user and group roles that have already been created. Click on the User or Group ± toggle to expand (or contract) the display of user or group roles.

- Assign a single role: Click on its name in the Available Roles box. Then click on the > button to move the role to the Selected Roles box. Repeat this process to assign additional roles individually. (The Selected Roles box also presents entries for User Roles, Group Roles, or both, as appropriate to your selections. Click on the User or Group ± toggle to expand or contract the display of user or group roles.)
- Alternatively, click on the >> button to move all roles to the Selected Roles box.
- If you reconsider your choices, select roles individually in the Selected Roles box and click on the < button to return them to the Available Roles box. Alternatively, click on the << button to return all roles to the Available Roles box.

4. Save the role. Click on the Save button to save the role and reopen it in an Edit Role page. Or click a Save and Close button to save the role and return to the Role Administration page. (Alternatively, click a Cancel button to return to the Role Administration page without saving the values you've configured.)

The Datasource, Business Objects, and Page Access panes are visible, but these panes are read-only because the group role inherits properties from its constituent roles. You cannot enter vales in them. As was true of user roles, you can select members (users) for a group role only indirectly by assigning the role to users in the User Administration page.

Editing Roles

To edit roles:

1. In the Roles pane of the Role Administration page, click on the row for the role you want to edit.
2. Click on Actions > Edit. Or click on the Edit icon, which looks like a pencil. An Edit Role page opens. It's a replica of the (user or group) Create Role page, except that it displays values already configured for the role you want to edit.
3. Using procedures described for creating a either a user or group role, modify the any of the settings for the role.
4. Save the role. Click on the Save button to save the role and reopen it in the Edit Role page. Or click Save and Close to save the role and return to the Role Administration page. (Or, click Cancel to return to the Role Administration page without saving the role values you've configured.)

Duplicating Roles

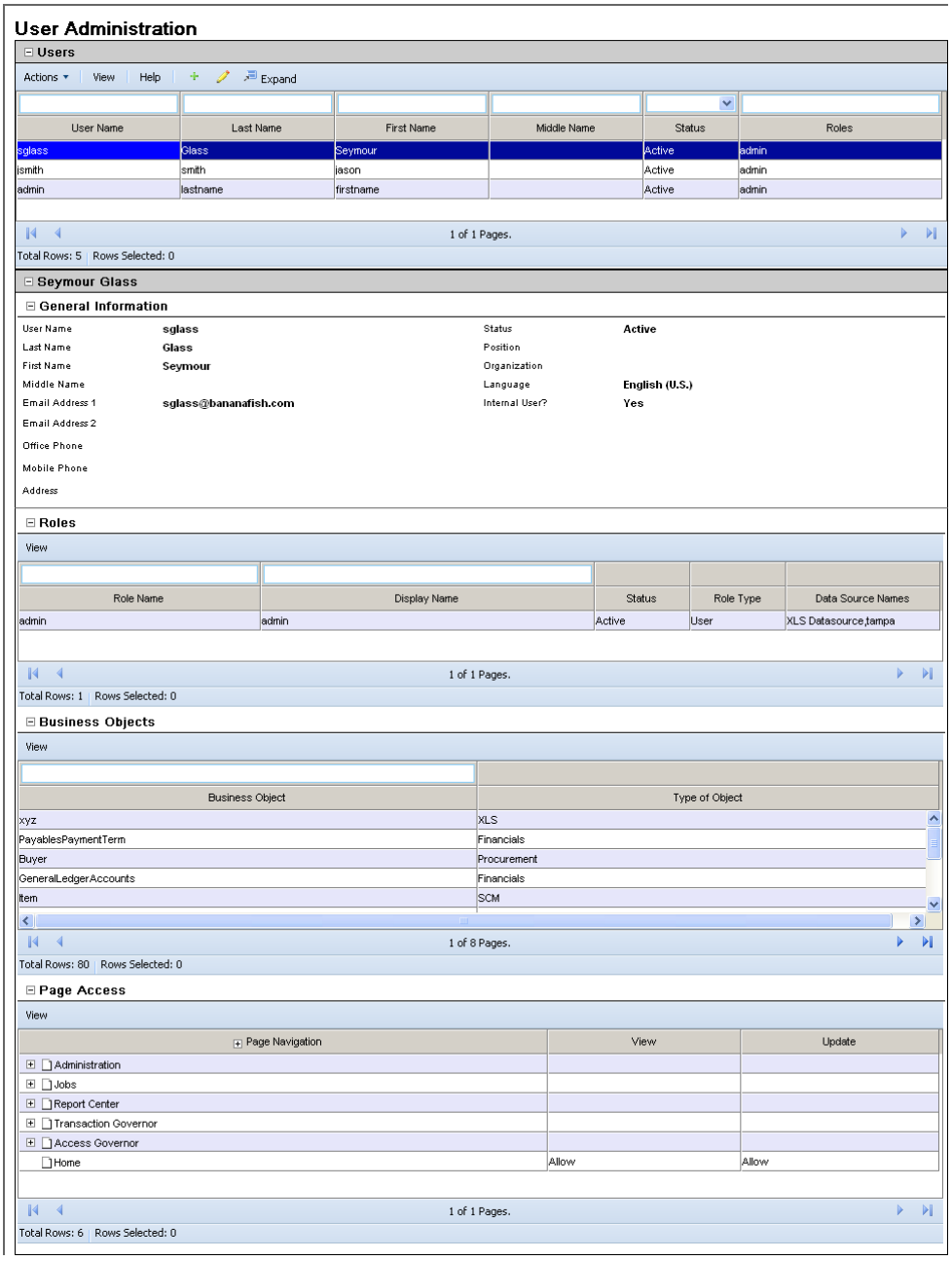
Rather than create a role from scratch, you can copy an existing role, then modify the copy:

1. In the Roles pane, click on the row for the Role you want to copy.
2. Click on Actions > Duplicate. Or click on the Duplicate icon, which looks like one page layered on top of another.

3. The Create Role page opens, displaying all values configured for role you are copying except for Role Name and Display Name. Type values in these fields to distinguish the copy you're creating from the original.
4. Modify other values as you see fit, and save the role. (See "Create a User Role" or "Create a Group Role" for detailed procedures.)

Viewing User Accounts

To view or work with GRCC users, open a User Administration page — select the User Administration option in the Administration node of the Navigation panel.



The User Administration page provides information, in read-only format, about GRCC user accounts. Its upper pane, labeled “Users,” displays a list of existing user accounts, together with summary information about them — the user name (by which the user identifies herself as she logs on); the user’s given, middle, and surnames; the user’s status (active, inactive, or locked; see below); the GRCC roles assigned to her; and whether she is an internal user (created directly in GRCC or in an external source; see page 2-8).

In the Users pane, select (click on) the row for a user whose information you wish to review. A lower pane, labeled with the selected user’s given and surnames, displays detailed information about the user. This pane is divided into four parts:

- General Information displays the user’s name, email and physical addresses, and other identifying information entered as the user’s account was created or edited.
- Roles lists the GRCC roles assigned to the user as her account was created or edited, together with summary data about them.
- Business Objects lists the business objects to which the user’s roles give her access.
- Page Access displays a grid that expands to show all pages available in GRCC. (Entries in the grid mimic the hierarchy of the Navigation panel; click on the ± toggles to expand or contract levels in the hierarchy.) The grid also shows the user’s access to these pages, as granted by her roles: For each page, View and Update privileges are labeled either *Allow* or *Deny*.

Creating User Accounts

To create a user account:

1. In the User Administration page, click on Actions > Create New. A Create User page opens.
2. Enter values in the General Information 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 User Name field, type a name by which the user identifies herself as she logs on. A user name 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. GRCC uses this address to send notifications to the user when she is assigned tasks for review.
    - Optionally, provide tracking information — a second email address, office and mobile phone numbers, physical address, and the user’s position and organization — in the appropriate fields.
    - In the Status field, select a status for the user — typically Active. You would select Inactive if a user is no longer eligible to use GRCC (for example, if

the user resigns from your company). You can also select Locked, although typically this status is set automatically by GRCC if the user fails to log on properly after five attempts (see “Editing or Unlocking User Accounts“ on page 2-9).

- In the Language field, select a language in which GRCC will display information when the user logs on. An administrator uses the Application Configuration page to select languages from among a set of eleven in which GRCC can display information. (See “Setting Properties” on page 3-7). This field enables you to choose one language from among that administrator’s selection. (The user can override this setting, either temporarily by selecting a language as he logs on, or permanently by selecting a new default language while configuring a user profile.)
- In the Password field, type a password with which the user validates her user name 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 user name.

  The user’s password expires every 90 days. When the password expires, the user is prompted to create a new one as she logs on. The new password must not match any of the previous three passwords.
- An Internal User value is updated by GRCC. It reads *Yes* if the user account was created in GRCC, or *No* if it originated in a database that uses LDAP technology to share user information. An external user becomes an internal user when he is assigned a GRCC role; at that point, his Internal User entry changes to *Yes*.

3. Assign roles to the user.
   - The Roles section of the Create User page contains two boxes, one labeled *Available Roles* and the other *Selected Roles*. The Available Roles box displays entries for user roles (individual roles) and group roles (a set of two or more roles that confers all access defined by its member roles) that have been created in the Role Administration page. Click on the User or Group ± toggle to expand (or contract) the display of user or group roles.
   - Assign a single role: Click on its name in the Available Roles box. Then click on the > button to move the role to the Selected Roles box. Repeat this process to assign additional roles individually. (The Selected Roles box also presents entries for User Roles, Group Roles, or both, as appropriate to your selections. Click on the User or Group ± toggle to expand or contract the display of user or group roles.)
   - Alternatively, click on the >> button to move all roles to the Selected Roles box.
   - If you reconsider your choices, select roles individually in the Selected Roles box and click on the < button to return them to the Available Roles box. Alternatively, click on the << button to return all roles to the Available Roles box.

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 User Administration page. (Alternatively, click a Cancel button to return to the User Administration page without saving the user account values you've configured.)

Although the User Administration page displays the business objects and GRCC pages available to a user, you cannot select these items directly in the Create User page. You can modify these selections only indirectly, by changing the assignment of roles to the user or by modifying roles in the Role Administration page.

Editing or Unlocking User Accounts

To edit a user account:

1. In the Users pane of the User Administration page, click on the row for the user account you want to edit.
2. Click on Actions > Edit. An Edit User page opens. It's a replica of the Create User page, except that it displays values already configured for the user whose account you want to edit.
3. Using the procedures described for creating a user, modify the General Information settings, Roles settings, or both for the user.

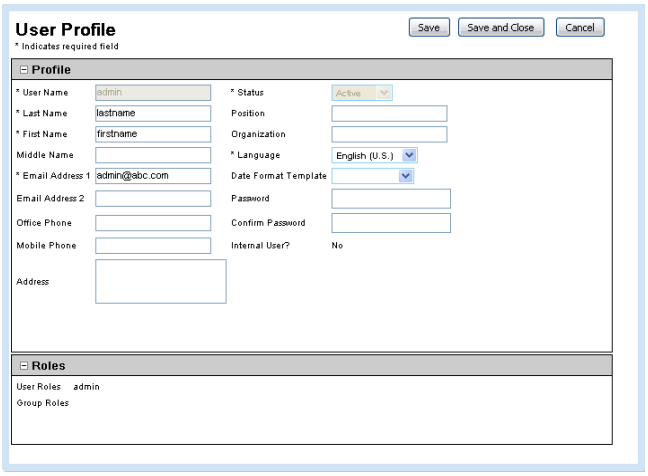
   You cannot, however, edit the User Name field. To change a user name, set the existing account to the Inactive status, and create a new account. Moreover, once again, you cannot directly edit business objects or GRCC pages available to a user, even though these are displayed in the User Administration page. You can modify these selections only indirectly, by changing the assignment of roles to the user or by modifying roles in the Role Administration page.
4. Save the user account. Click on the Save button to save the account and reopen it in the Edit User page. Or, click a Save and Close button to save the account and return to the User Administration page. (Alternatively, click a Cancel button to return to the User Administration page without saving the user account values you've configured.)

If a user fails to log on in five consecutive attempts, GRCC 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.

Modifying Your Own User Account

From any page in GRCC, the user who is currently logged on can open a User Profile. In it, he can review information pertaining to his own user account and change some of it, even if he does not have update rights to the User Administration page.

To open the User Profile, click on the Profile link near the upper-right corner of GRCC (in the dark blue band that runs along the top of the application). A User Profile dialog appears (as shown at the top of the next page).



In read-only fields, the User Profile displays the username, status, and roles assigned to the user. It also shows whether the user is an "internal user." (The value *No* indicates that the user account originated in a database that uses LDAP technology to share user information; the value *Yes* indicates that the account was created in GRCC, or was created externally but then assigned a GRCC role.) These values cannot be changed.

The User Profile dialog includes write-enabled fields for the following information: first, last, and middle names; physical address; email and second email addresses; office and mobile phones; position and organization; and password. The password field is blank for security purposes, but all the others display current values.

To make changes to these fields, type new entries in them. (If you are changing your password, type the new one not only in the Password field, but also in the Confirm Password field.)

The two remaining fields enable you to set a language in which you wish to work:

- In the Language field, select the language. You can choose among languages that have been configured for use in the Application Configuration page.

  GRCC displays information in the language you choose here if you make no selection in a Language Preference field as you log on. If you do select a language as you log on, that selection overrides the one you make here. (If you make no selection in either place, GRCC uses, in order of preference, the language selected for your web browser or US English.)

- In the Date Format Template field, select a date format appropriate for the language in which you wish to work. If you make no selection, GRCC displays dates in its default format: *mm/dd/yyyy*.

When you finish setting user-profile options, save them: Click on the Save button or the Save and Close button. The former leaves profile values on display for further editing, and the latter closes the User Profile window. Alternatively, click on Cancel to close the window without saving new profile values.

3

Data Administration

Using tools available in the Administration area, you can configure connections between GRCC and instances of the business-management applications subject to its controls, set up GRCC to send email notifications to AACG policy participants, or set properties required for GRCC to connect to its database, to display information in varying languages, or to integrate with other applications. You can also import business objects for use with TCG models.

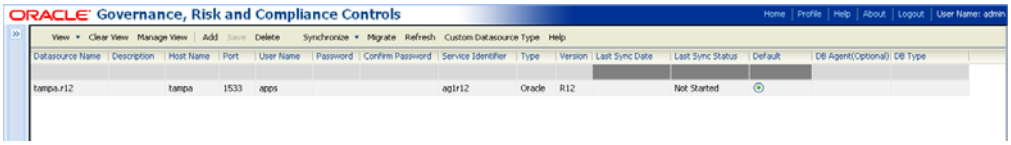
Working with Datasources

Governance, Risk and Compliance Controls works with data gathered from business-management applications. For it to do so, you must configure connections to datasources for instances of these applications. GRCC comes prepared for you to configure connections to Oracle or PeopleSoft datasources. If you intend to configure a connection to an instance of another business-management application, you must first configure a datasource type for that application. Once connections are established, you would periodically "synchronize" GRCC data with that in the datasources; there are distinct synchronization procedures for data used by AACG and data used by TCG.

Configuring a Datasource Connection

To configure a datasource:

1. Locate and click on the Data Administration entry under the Administration node in the Navigation panel. The following page opens:



2. Click on the Add button. A new row appears. To enter values in this row, double-click in each field (or press the Tab key to move from an active field to the next field). Enter the following values:

   - Datasource Name: Create a name for the datasource. (This name appears in the Datasource column of the AACG Access Point List window as you

select access points or entitlements for use in an access policy, or select access points for an entitlement. It also appears in the TCG Manage Datasource window as you use the Create Model page to build models.)

- Description: Type a brief description of the datasource (optional).
- Host Name: Supply the URL for the machine that hosts the database used by the business-management application.
- Port: Enter the port number that database uses to communicate with other applications.
- User Name: Supply the user name for the database used by the business-management application. For an Oracle database, this is the same as Schema Name (below); for an Oracle EBS instance, this is typically APPS.
- Password: Enter the password for the database.
- Confirm Password: Re-enter the password for the database.
- Service Identifier: Supply the service identifier (SID) for the database used by the business-management application.
- Type: From a list box, select the type of business-management application to which you are connecting — by default, Oracle or PeopleSoft. To set up other applications for selection in this list box, see "Configuring Datasource Types" on page 3-3. (The value you choose appears in the Platform column of the AACG Access Point List window as you select access points or entitlements for use in an access policy, or select access points for an entitlement.)

  Or, select AG Schema if you are configuring a connection to an earlier version of AACG, for use in migrating its access policies to your current version.
- Version: From a list box, select the version number of the business-management application to which you are connecting.
- Default: Select the radio button to designate a default datasource — one whose data is subject automatically to models as they are created in the TCG Model Workbench. Datasources *not* designated as default may be selected manually as sources of a model, but they are not designated automatically. The default datasource may be removed from any given model. There can be only one default datasource. The selection of a default datasource has no bearing on AACG access policies
- DB Agent: Tells the Oracle Data Integrator (ODI) agent to use DB Link on Oracle databases. Enter the DB Link name you've specified externally for the datasource. The use of this column is optional.
- DB Type: The type of database — Oracle or MS SQL Server — used by the ERP application being configured as a datasource.

3. When you finish entering values, click on the Save button in the tool bar.
4. After saving the datasource, click on the Refresh button in the tool bar. (This enables you to create global conditions for the datasource.)

You can edit an existing datasource by clicking on fields in its row and entering new values, or you can delete a datasource by clicking on its row and then clicking on the Delete button in the tool bar.

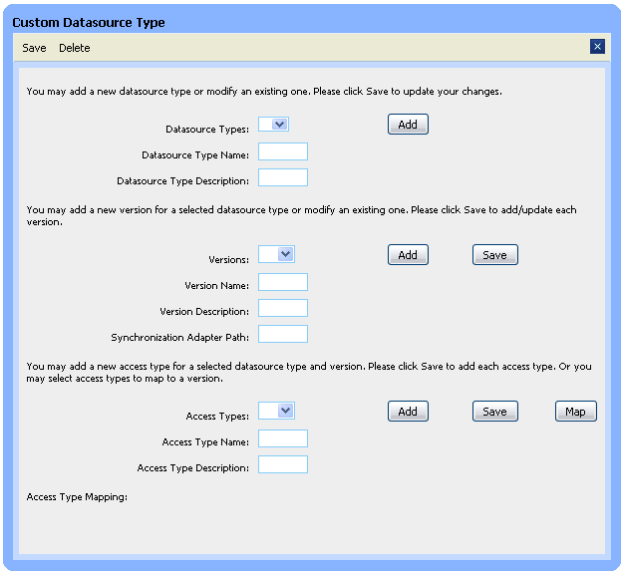
Configuring Datasource Types

To work with any given business-management application, AACG requires an "adapter." Conceptually, the adapter uses ETL (extract, transform, load) technology to collect information about users and access points in the business-management application, and to provide that information to AACG.

Adapters for Oracle E-Business Suite, PeopleSoft Enterprise, and earlier versions of AACG itself are built into AACG. Thus by default, the Type column in the Data Administration panel enables you to select the values *Oracle*, *PeopleSoft*, and *AG Schema* to use these adapters.

To configure other business-management applications as data types:

1. Click on the Custom Datasource Type button in the tool bar near the top of the Data Administration page. A Custom Datasource Type dialog opens.



2. Type a name for the datasource type in the Datasource Type Name field. (This is the name that will appear in the Type list box.) Also type a brief description in the Datasource Type Description field.
3. Click on Save in the tool bar at the top of the Custom Datasource Type dialog. (To save the values you've entered in the Type Name and Type Description fields, you must use the Save option at the top of the dialog, not either of the other two Save buttons.) A pop-up window displays the message "Datasource type saved successfully." Click on its OK button to clear it.
4. After the save operation, the Custom Datasource Type dialog closes. Reopen it by clicking once again on the Custom Datasource Type button in the tool bar near the top of the Data Administration page. Then select the type value in the Datasource Types list box.
5. In the Version Name and Version Description fields, enter values that set and describe the version of the datasource type you are creating.
6. In the Synchronization Adapter Path field, type the full path to the directory containing the adapter created for your business-management application.

7. Click on the Save button to the right of the Version and Adapter fields. (You must select this button to save the information entered in these fields.) The save operation blanks these fields. Repopulate them by selecting the version you have just saved in the Versions list box.
8. In the Access Type Name field, type a name recognized by your adapter for a type of access point in the business-management application (for example, "Function" rather than any particular function). Also enter a brief description in the Access Type Description field. Click the Save button to the right of the Access Type fields. Repeat this step for all other access points you want to make available for use in access policies.
9. Map access points to your version: in the Access Types list box, select one of the values you created step 8, and click on the Map button. The value appears in the read-only Access Type Mapping field at the bottom of the dialog. Repeat this process for all other access points you want to map to your version.

To edit custom datasource types, select existing values in the list boxes; each selection in a list box populates its associated fields. Values appear for selection in a given list box only after a selection has been made in its parent list box — for example, nothing is available in the Versions list box until you make a selection in the Datasource Types list box. When fields are populated, you can modify their contents and save the changes. When fields are blank, you can add new values and save them. If you select any of the Add buttons, you remove the contents of the corresponding fields so that you can add new values.

Synchronizing Data

To capture changes made in business-management applications over time, synchronize their data with the data used by AACG or TCG:

1. Select the row for the datasource with which you want to "synchronize data" — capture changes made in business-management applications since the last time the data-synchronization process was run. You may select more than one row (holding down the Shift or Ctrl key to select rows either in or out of sequence).
2. Click on the Synchronize button in the tool bar. A two-item list appears; in it, click on Run Now or Schedule.
    - If you select Run Now, a submenu offers two options. Click on Access to synchronize data used by AACG, or on Transaction to synchronize data used by TCG. A pop-up dialog asks you to confirm that you want to run the synchronization process. Click its OK button to do so.
    - If you select Schedule, a dialog opens. Select the Access or Transaction check box to synchronize data used by AACG or TCG (or select both), and enter values that set the name of the schedule, its start date, the regularity with which the synchronization should occur, and an end date (if any). Then click on the Schedule button.

Migrating Policies from One Datasource to Another

You can migrate access policies from one AACG instance to another:

1. Ensure that both source and destination instances are configured as datasources.

2. In the Data Administration page, click on the row for the destination instance, which must be one whose Type value is set to *AG Schema*.
3. Click on the Migrate button in the tool bar of the Data Administration page. A Migrate Policies pop-up window appears.
4. In the field on the left, click on the version of AACG from which you want to migrate policies. This populates the field on the right with instances of that version that you have configured as datasources.
5. Click on the instance whose policies you want to migrate. Then click on the Migrate button.
6. A pop-up message reports the number of policies migrated and the status of the migration operation. Click on its OK button to clear it.

Configuring Notifications

In the AACG Definition panel, users may be named as policy participants. In the AACG Work Queue, users may be assigned to review conflict paths. These users may receive notification via email when conflicts require their attention. To activate notification, establish a connection with your SMTP server, and then either send notifications manually or schedule them to be sent by AACG.

To do either, open the Notification Configuration page. In the Navigation panel, click on the Notification Configuration link under the Administration node.

Connecting to Your SMTP Server

The Notification Configuration page contains a single row in which you enter information about the SMTP server your company uses for sending email. Application Access Controls Governor uses your email system to send notifications to policy owners or observers, or to users assigned to review conflict paths, when conflicts are generated.

To enter values in the row, double-click in each field (or press the Tab key to move from an active field to the next field). Enter the following values:

- SMTP Host: The host name for the SMTP server your company uses for sending email.
- Port Number: The port number at which the SMTP server communicates with other applications.
- User: The user name with which one would log on to the SMTP server. This value is required only if access to the SMTP server requires authentication.
- Password: The password with which one would log on to the SMTP server. This value is required only if access to the SMTP server requires authentication.
- 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 Application Access Controls Governor. This takes the form `http://host:port/ags`, in which *host* is the fully qualified domain name of your GRCC server, and *port* is the value you

have configured as your “Tomcat port.” (GRCC uses the Tomcat Application Server to run. By default, the Tomcat port number is 8080.)

- SSL Authentication: Select this check box if access to your SMTP server requires authentication; clear the check box if it does not. If authentication is required, the User and Password fields must also be populated (see above).
- Active: Select this check box to activate the sending of notifications, or clear it to inactivate the sending of notifications.

When you have finished entering values, click on the Save button. If you have cleared the Active check box, a pop-up message alerts you that all queued notifications will be purged, and prompts you to confirm your choice. Click on its OK button to continue.

Sending Notifications

You can send notifications manually, or schedule them to be sent:

1. In the Notification Configuration panel, click on the Schedule button.
2. A Schedule Parameter dialog appears. In it, do either of the following:
   - In its Start Date fields, enter a date and time (in the format *hh:mm*) at which GRCC should begin to send notifications. In its Every field, enter the interval (in hours) at which notifications should be sent. Then click on the Schedule button.

     At each scheduled interval, GRCC consolidates queued notifications so that each reviewer receives one message for the conflict paths awaiting his review.
   - Click on the Run Now button. Queued notifications are consolidated and sent once. To use this option, you need not enter values in the Start Date and Every 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.

Application Configuration

The Application Configuration page contains five tabs:

- Properties sets parameters required for GRCC to connect to its database.
- Analytics Integration enables GRCC to supply data to Oracle Business Intelligence Publisher (BIP), in which you can create custom AACG reports, or to Governance, Risk and Compliance Intelligence (GRCI), another Oracle product.
- User Integration sets up GRCC to recognize users created externally in a database that uses LDAP technology to share user information.
- Patterns uploads patterns (statistical functions) that may be used in TCG models.
- Maintenance purges AACG conflict-analysis runs.

To open the Application Configuration panel, select Application Configuration under the Administration node of the Navigation panel.

Setting Properties

The Properties tab opens a panel that sets values required for Governance, Risk and Compliance Controls to connect to its database. Typically, you would accept values set during installation, and would use this panel to update the values only if your configuration needs to change. To set these properties:

1. Click on the Properties tab.
2. In the GRCC Schema section of the Properties page, type or select the appropriate value for each property:
   - User Name: Supply the user name for the GRCC database.
   - Password: Supply the password for the GRCC database.
   - Confirm Password: Re-enter the password for the GRCC database.
   - Port Number: Supply the port number at which the GRCC database server communicates with other applications.
   - Service Identifier: Supply the service identifier (SID) for the GRCC database server.
   - Server Name: Supply the fully qualified domain name of the database server.
   - Report Repository Path: Supply the full path to your Report Repository. This is a directory, established during installation, that stores report history.
   - Log Threshold: Select a value that sets the level of detail in log-file entries. From least to greatest detail, valid entries are *error*, *warn*, *info*, and *debug*.
   - Transaction ETL Path: Enter the full path to a directory created during GRCC installation to hold ETL data used by Transaction Controls Governor.
3. In the Performance Configuration section of the Properties page, select or clear options that may optimize GRCC performance.
   - Externalize Report Engine: Select the check box to enable the reporting engine to run in its own java process, so that the generation of very large reports does not affect the performance of other functionality. However, select the check box only if you have installed GRCC on hardware that is identified as as “recommended” in the *Governance, Risk and Compliance Support Matrix*; clear the check box if you use “supported” hardware.
   - Optimize Distributed Operation: Select the check box to increase the speed at which GRCC performs distributed operations such as data synchronization. However, for this selection to have any effect, at least one datasource (configured in the Data Administration page) must have an entry in its DB Agent field. (This entry, in turn, is a DB Link name configured externally to GRCC.) The Optimize Distributed Operation setting enhances performance only in GRCC exchanges with datasources with values entered in the DB Agent field.
   - Optimize Appliance-Based Operation: Select the check box to optimize performance if the GRCC application and GRCC schema reside on the same machine. Do not select this check box if the GRCC application and

schema do not reside on the same machine. If you select this check box, you must enter a value in the ORACLE_HOME Path field.

When you select the Optimize Appliance-Based Operation field, 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 GRCC schema.

- Enable Era-Based ETL Optimization: Select this check box to cause TCG data synchronization (see page 3-4) to operate only on data entered in business-management applications after a specified date. (This setting has no impact on data synchronization operations for AACG.)

  When you select the Enable Era-Based ETL Optimization field, and Analysis Start Date field appears. In it, enter a date from which you want synchronization runs to recognize data changes. 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.

4. To choose languages available to GRCC users, select their check boxes in the Language Preferences section of the Properties page. (Or, clear check boxes to make languages unavailable.) Once selected here, languages are available for selection by individual users as they configure their user profiles or as they log on to GRCC.
5. When you finish entering property values, click on the Test button.
6. GRCC determines whether the property values enable it to connect to its database and read the directory path for the Report Repository.
   - If not, you have entered an incorrect value for at least one of the properties. Examine the values, make corrections, and click the Test button once again.
   - If so, the property values are correct and a Save button becomes active. Click on that button to save your settings.
7. In response to a prompt, restart the server.

A section titled Web Services Authentication contains a single field, Use Basic Authorization. GRCC can be integrated with an application whose database shares its user information through LDAP technology. However, there are limitations that could materially affect existing data and functionality. Therefore, this should be done in conjunction with professionals experienced in this type of integration for GRCC. Contact Oracle Consulting Services or another experienced organization for assistance.

Setting Up Analytics Integration

Oracle-supplied report templates enable users to develop custom AACG reports that run in Oracle Business Intelligence Publisher, or BIP. (These reports, and the templates from which they are derived, are distinct from the reports that are supplied with GRCC, and that run in its Report Center.) In addition, GRCC can supply data to Governance, Risk and Compliance Intelligence (GRCI), another Oracle product.

In either case, GRCC must place data in a schema distinct from its principal one, and from which either BIP or GRCI reads data; it’s known as the “data analytics”

schema. To implement the report templates or GRCI connectivity (or both), create the data analytics schema, then use fields in the Analytics Integration tab to set values that identify the data analytics schema.

The data analytics schema should reside on a server distinct from the one on which the GRCC schema runs, and should use a distinct tablespace. The following is a sample script for creating the data analytics schema in an Oracle 10g or 11g database. Assume you have created the data analytics tablespace (called *ag_access_tablespace* in the script) and that the schema (user) name and password are *ag_access_user* and *ag_access_password*.

```
create user ag_access_user identified by ag_access_password
default tablespace ag_access_tablespace quota unlimited on
ag_access_tablespace quota 0k on system;
grant connect, resource to ag_access_user;
grant create any view to ag_access_user;
grant create any table to ag_access_user;
grant drop any table to ag_access_user;
```

Moreover, if you use an Oracle 10g or 11g database, execute these commands, then bounce the database:

```
ALTER SYSTEM SET open_cursors=1000;
ALTER SYSTEM SET processes=400 scope=spfile;
ALTER SYSTEM SET sessions=600 scope=spfile;
```

If you choose to use the system tablespace, rather than create one specifically for data analytics, simply delete the phrase “default tablespace ag_access_tablespace quota unlimited on ag_access_tablespace quota 0k on system” from the script.

If your GRCC instance is an upgrade from an earlier 8.*x* version of AACG, use the data analytics schema created for the earlier version. Note, though, that earlier versions supported the Oracle 9i database, but GRCC 8.5.1 does not. If you used 9i with your earlier version, upgrade to a supported (10g or 11g) database. Before upgrading, take a backup of your schema.

If you wish to use the multilingual capabilities of GRCC, be sure the database that hosts the data analytics schema is set up for UTF-8 encoding. Specifically, the character set should be set to AL32UTF8. Refer to your Oracle Admin guide for information on verifying or configuring your database with the recommended character set.

Once you have created the data analytics schema, use the GRCC Application Configuration page to connect GRCC to the schema:

1. In the GRCC Application Configuration page, click on the Analytics Integration tab.
2. Type or select the appropriate value for each property:
    - User Name: Supply the user name for the data analytics schema.
    - Password: Supply the password for the data analytics schema.
    - Confirm Password: Re-enter the password for the data analytics schema.
    - Port Number: Supply the port number at which the database server communicates with other applications.
    - Service Identifier: Supply the service identifier (SID) for the database server.

- Server Name: Supply the fully qualified domain name of the database server.
- Run Analytics: Select the check box to enable the sharing of data.

3. When you finish entering property values, click on the Test button.
4. GRCC determines whether the property values enable it to connect properly.
   - If not, you have entered an incorrect value for at least one of the properties. Examine the values, make corrections, and click the Test button once again.
   - If so, the property values are correct and a Save button becomes active. Click on that button to save your settings.
5. In response to a prompt, restart the server.

The data analytics schema is updated each time conflict analysis is run in Application Access Controls Governor. (For more on conflict analysis, see "Purging Conflict Runs" on page 3-11.)

Setting User Integration Properties

GRCC can be integrated with an application whose database shares its user information through LDAP technology. However, there are limitations that could materially affect existing data and functionality. Therefore, this should be done only in conjunction with professionals experienced in this type of integration for GRCC. Contact Oracle Consulting Services or another experienced organization for assistance.

1. Click on the User Integration tab.
2. In the Single Sign On section, select the Enable Single Sign On check box to make use of Single Sign On, which establishes a single set of log-on credentials for each user in varying applications. (Or, clear the check box if you do not wish to use Single Sign On.)
3. In the External LDAP User Repository section, type or select an appropriate value in the field corresponding to each property:
   - Enable Integration: Select the check box to permit user integration to occur.
   - Hostname: Enter the host name of the LDAP database server.
   - Port Number: Supply the port number at which the LDAP database server communicates with other applications.
   - User Name: Supply the user name for the LDAP database schema.
   - Password: Supply the password for the LDAP database schema.
   - Confirm Password: Re-enter the password for the LDAP database schema..
   - Bind DN Suffix: Supply the common suffix added to each user ID to form the LDAP Bind DN. (Each user must have a UID attribute).
   - Users Organizational Unit: Supply the "container" in the LDAP hierarchy that holds user records.
4. When you finish entering property values, click on the Test button.

5. GRCC determines whether the property values enable it to connect properly.
    - If so, the property values are correct and a Save button becomes active. Click on that button to save your settings.
    - If not, you have entered an incorrect value for at least one of the properties. Examine the values, make corrections, and click the Test button once again.
6. In response to a prompt, restart the server.

Uploading Patterns

"Patterns" are statistical functions, supplied by Oracle, that may be used in the creation of Transaction Controls Governor models. Independently of GRCC releases, Oracle may issue files (in .jar format) that contain patterns. To upload these files:

1. Click on the Patterns tab.
2. Click on Action > Upload File.
3. An Upload Pattern pop-up window opens. Click on its Browse button.
4. A Choose File dialog opens. In it, use standard Windows techniques to 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 Upload Pattern 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 Upload Pattern window.

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

Purging Conflict Runs

From the AACG Definition page (in which access policies are created or edited) or the Conflict Analysis page (in which conflicts may be reviewed), a Find Conflicts program may be run. It evaluates business-management-application users, noting those whose work assignments violate access policies. In the Work Queue, AACG users may be assigned to review paths that lead to conflicting access points, and those users may assign status.

Each Find Conflicts run generates a distinct set of results. The Conflict Analysis page and the Work Queue may display the results of individual runs, or may display a cumulative set. In the latter case, each conflict identified in multiple runs is displayed once. So that this display is current, each time the Find Conflicts program is run, Work Queue settings from the most recent run — assignments of paths to reviewers, statuses, and the dates on which statuses were set — are copied forward into the new run.

You can purge individual runs of the Find Conflicts program. If a purge removes all record of a conflict, but the conflict continues to exist (it involves access points that at least one user can still reach), the next run of the Find Conflicts program will, of course, find that conflict once again. However, Work Queue settings are retained only if the Find Conflicts program is run *before* the earlier run of the program is

purged. As a result, the purge procedure prompts you to run Find Conflicts before executing a purge.

A simulation feature enables users to forecast the effects of conflict cleanup. If you purge a set of conflict results upon which a simulation had been based, rerun the simulation to update its results.

To purge runs of the Find Conflicts program:

1. Click on the Maintenance tab.
2. From a list titled “Access Conflict Analysis Runs,” select runs you wish to purge. To select one, 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 runs. The list is sorted by date, with the oldest conflict run first and the most recent last. You can filter the list by date.
3. A check box labeled “Run conflict analysis prior to purge” is selected by default. Leave it selected to run the Find Conflicts program before purging, and thus ensure that Work Queue settings are retained for all conflicts. Clear it only if you do not wish to retain Work Queue settings.
4. Click on the Purge button.
5. A confirmation message appears. Click on its OK button.

Uploading Business Objects

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

To complete a business object upgrade, you would 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 upload business objects:

1. Open the Business Object Administration page. Select Business Object Administration under the Administration node of the Navigation panel.
2. To import a business object dictionary file, click on Actions > Import Business Object Dictionary. To import a business object mapping, click on Actions > Import Business Object Mapping. To import business objects, 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 Choose File dialog opens. In it, use standard Windows techniques to 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 import operation is complete, a row presenting summary information about it appears in the Business Objects grid.

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.

4

Jobs Administration

"Jobs" are programs that synchronize data, find AACG conflicts, run TCG models and export results, generate reports, and perform other background tasks. Some jobs can be run on demand, or can be scheduled to run. In general, you would run or schedule a job in a page to which it applies — for example synchronize data in the Data Administration page or find conflicts the AACG Definition page.

However, Jobs Administration panels enable you to view job histories, or review schedules of jobs that are set to be run in the future. Users with update privileges to the Jobs Administration panels can also revise the schedules of jobs that are yet to run.

Viewing Job History

To view a history of both scheduled and on-demand jobs, expand the Jobs entry in the Navigation panel, and then click on its Job History link. The following Job History panel appears:

Each row presents the following information about one occasion when a job is run:

- Job ID: An identification number assigned internally to the job by GRCC.
- Name: The Name of the job that was run.

- Start Date and End Date: The dates and times on which the job began to run and finished running.
- Status: The current state of a job. Most statuses are assigned by GRCC. These include Not Started, Started, Queued, Pause Requested, Paused, Completed, and Error. GRCC updates the status until a final state (either Completed or Error) is reached.

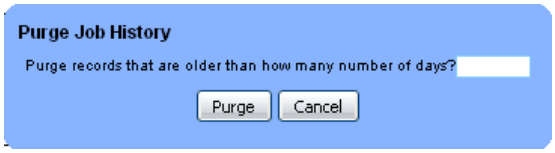
  GRCC prioritizes jobs: TCG model analysis, AACG conflict analysis, and AACG simulation have highest priority, followed by data synchronization, followed by all others (such as running reports). The Pause (or Pause Requested) status indicates that GRCC has suspended (or is attempting to suspend) a job in order to undertake a higher-priority job. Only GRCC can pause jobs or request that they be paused; there is no way for a user to do so.

  Users may, however, cancel jobs (see "Canceling Jobs," below). When a user does so, the job status changes to Cancel Requested or, ultimately, to Canceled.
- Message: An informational message about the job status.
- Run By: The user name of the user who ran the job.

Purging Jobs

If you have update permission to the Job History 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.



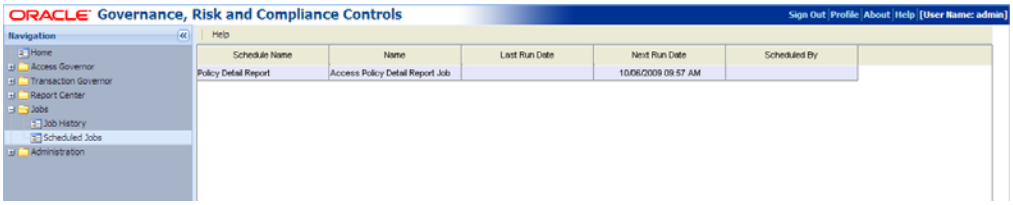
2. In the "days old" field, enter a number of days before the present date. This effectively defines a new date; jobs completed after that date are kept, and those completed before that date are deleted. For example, if the current date is July 30 and you enter the value 1, your purge date is July 29 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.

Canceling Jobs

If you have update permission to the Job History 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.

Viewing and Resetting Job Schedules

To view schedules for jobs that are yet to be run, expand the Jobs entry in the Navigation panel, and then click on its Scheduled Jobs link. The following Scheduled Jobs panel appears:



Each row presents the following information about a job scheduled to run in the future:

- 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 GRCC user who created the schedule.

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

1. Double-click on the row for a schedule. Its Schedule Parameter dialog opens. Each schedule is specific to the type of job being scheduled, and each dialog is specific to the schedule it 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.