

Oracle® Application Access Controls Governor

User Guide

Release 8.6.4.8000

Part No. E41919-01

August 2013

Oracle Application Access Controls Governor User Guide

Part No. E41919-01

Copyright © 2013 Oracle Corporation and/or its affiliates. All rights reserved.

Primary Author: David Christie

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

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

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

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

U.S. GOVERNMENT RIGHTS

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

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

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

Contents

1 Introduction

| | |
|---|-----|
| AACG Models and Controls..... | 1-1 |
| Incident Analysis..... | 1-2 |
| Reporting..... | 1-4 |
| Common Procedures..... | 1-4 |
| Selecting Perspectives..... | 1-4 |
| Synchronizing Data..... | 1-6 |
| Attaching Files..... | 1-6 |
| Importing and Exporting CCM Elements..... | 1-7 |

2 Creating and Managing Models

| | |
|---|------|
| Managing Models..... | 2-1 |
| Viewing Models..... | 2-2 |
| Creating, Editing, Copying, or Deleting Models..... | 2-2 |
| Model-Data Synchronization..... | 2-2 |
| Creating an Access Model..... | 2-3 |
| Naming the Model..... | 2-3 |
| Selecting Business Objects..... | 2-3 |
| Selecting Datasources..... | 2-5 |
| Arranging Filters..... | 2-6 |
| Creating an Access Point or Entitlement Filter..... | 2-8 |
| Creating a Condition Filter..... | 2-9 |
| Saving the Model..... | 2-11 |

| | |
|--|------|
| Managing and Creating Global Conditions..... | 2-11 |
| Creating Global Conditions..... | 2-11 |
| Editing or Copying Global Conditions..... | 2-12 |
| Managing and Creating Entitlements | 2-13 |
| Creating an Entitlement..... | 2-13 |
| Adding Access Points to an Entitlement..... | 2-13 |
| Editing an Entitlement..... | 2-14 |
| Copying an Entitlement | 2-15 |
| Managing and Creating User Defined Access Points..... | 2-15 |
| Using Path Conditions..... | 2-16 |
| Viewing or Exporting Model Results..... | 2-17 |
| Visualizing Access Results | 2-18 |
| 3 Creating and Managing Continuous Controls | |
| Creating Access Controls..... | 3-1 |
| Naming and Describing Controls..... | 3-2 |
| Setting Priority, Status, Result Type, and Enforcement Type | 3-2 |
| Selecting Datasources..... | 3-3 |
| Selecting Perspective Values and Result Investigators..... | 3-3 |
| Writing Comments..... | 3-4 |
| Mass-Editing Controls..... | 3-4 |
| Viewing and Editing Individual Controls | 3-4 |
| Running Controls | 3-5 |
| Contextual Reporting for Controls..... | 3-6 |
| 4 Resolving Incidents | |
| Viewing Controls or Incidents in Summary..... | 4-2 |
| Mass-Editing Incidents..... | 4-3 |
| Viewing and Editing Individual Incidents | 4-3 |
| Assigning Incidents | 4-4 |
| Assigning Relationships..... | 4-6 |
| Visualizing Access Incidents | 4-7 |
| Contextual Reporting for Incident Results..... | 4-7 |

| | |
|---|------|
| Using Access Simulation | 4-9 |
| Creating and Naming a Simulation | 4-9 |
| Creating a Simulation Model | 4-10 |
| Developing Remediation Steps | 4-11 |
| Running the Simulation and Viewing Results..... | 4-12 |
| Printing or Saving a Remediation Plan..... | 4-13 |

5 Managing Access Approvals

| | |
|---|-----|
| Assigning Responsibilities in Oracle EBS..... | 5-2 |
| Assigning Roles in PeopleSoft..... | 5-2 |
| Responding to Notifications | 5-3 |
| Viewing Access Approvals History | 5-4 |

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 *Application Access Controls Governor User Guide* covers features specific to AACG. (Other product-specific user guides cover features particular to ETCG and to EGRCM.)

An *Enterprise Governance, Risk and Compliance User Guide* covers most functionality common to the GRC applications (although the *Enterprise Governance, Risk and Compliance Installation Guide* covers some setup and administration topics). Refer to these guides as well as the AACG user guide as you use AACG.

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 begin to use GRC.

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 life cycle 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 life cycle of your software from planning through implementation, testing, production, and changes. In Oracle Fusion Applications, you can use the Oracle Enterprise Repository for:

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

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

Documentation Accessibility

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

Comments and Suggestions

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

Introduction

Oracle Application Access Controls Governor (AACG) enforces segregation of duties in Oracle E-Business Suite, PeopleSoft, and (if a “connector” is installed) Oracle Fusion Applications. AACG implements “models” and “controls” that define conflicts among duties assigned in a company’s applications and identify users who have conflicting access to those duties.

AACG is one of a set of applications, known collectively as “Oracle Advanced Controls,” that regulate activity in business applications. Together with another Advanced Controls application — Enterprise Transaction Controls Governor — AACG runs as a Continuous Control Monitoring (CCM) module in an Enterprise Governance, Risk and Compliance (GRC) platform.

AACG Models and Controls

An AACG model returns “temporary” results — a snapshot of risk that is replaced each time the model is evaluated. A control returns “permanent” results — records of violations that remain available to be resolved no matter how often the control is run.

A user creates a model, and may then convert the model into a control; users cannot create controls directly. Although the creation of a model is a preliminary step in the creation of a control, models may be created to run on their own, so that users such as auditors can assess the risk inherent in a system at a given moment.

An AACG model or control defines conflicts among “access points” in a company’s systems. An access point is an object in a business-management application which, when made available to a user, enables him to view or manipulate application data. Access points may be gathered into sets called “entitlements,” and a model or control may define conflicts among individual access points, those included in entitlements, or both.

Access points conflict when, in combination, they would enable individual users to complete transactions that may expose a company to risk. For example, distinct functions in Oracle EBS enable users to initiate a purchase order and to approve payment on that purchase order. In general, individual users should not be able to do both, so a model or control may be created to define the functions as conflicting.

A model, or a control into which the model is converted, consists of “filters.” Each selects business-management-application users who have been assigned a specified access point, or who have been assigned any of the access points in a specified entitlement. Within a model, any number of filters may be defined. For a conflict to exist, a user must be selected by a specified combination of those filters; that is, the user must be assigned the access points named in that combination of filters.

Each filter cites a “business object,” an “attribute” of that object, and a value for that attribute; these supply access data for analysis. Every AACG model uses an Access Point business object, an Access Entitlement business object, or both. The Access Point business object includes a Name attribute, for which values include the access points available in an application. The Access Entitlement business object also includes a Name attribute, for which values include entitlements configured by AACG users.

In addition, filters may serve as “conditions,” which define circumstances under which the control is enforced. Typically, they select users or other objects (such as companies in PeopleSoft or operating units in Oracle EBS) that are exempt from the control. Additional business objects supply values for use in creating conditions.

Records of control violations are known as “incidents.” Each control names one or more AACG users as “result investigators” who are responsible for resolving incidents.

Moreover, each AACG control is assigned one of three “enforcement types” — Prevent, Monitor, or Approval Required. The enforcement types determine what actions a result investigator may take when the control identifies incidents. Distinctions among these types are explained in “Incident Analysis” (below).

Users may create perspectives, each of which is a set of hierarchically arranged values. Each represents a context in which models, continuous controls, and incidents exist. Users can relate individual perspective values to individual models, controls, or incidents, thus cataloging them by organization, region, or any other concept the company finds meaningful. Perspective values also play a part in GRC security. In particular, perspective values associated with controls or incidents determine which users are eligible to be result investigators — those assigned data roles with matching perspective values.

Incident Analysis

Typically, continuous controls generate incidents when they are run (although specially configured controls may compile datasets for user defined objects). Each AACG incident traces the path through which a user of a business-management application, assigned access points that a control defines as conflicting, can reach one of those access points.

Each incident identifies a “privilege” (an access point actually included in a control) and a “role” (the level of object actually assigned to a user). Depending on how a control is configured, these may be a single object — for example, an Oracle EBS responsibility, if the control sets one responsibility in conflict with another. More commonly, however, they are distinct objects — for example, the role might be an Oracle EBS responsibility, and the privilege might be a function available within that responsibility. In such a case, the incident would identify not only the role and the privilege, but also the objects that lead from one to the other — in the Oracle EBS example, menus and submenus that lead from a responsibility to a function.

AACG can either discover conflicts that existed before controls were written to protect against them (“detective” analysis), or intervene when a user is assigned duties after controls have been written to define them as conflicting (“preventive” analysis). Incidents identified through detective analysis are displayed in a Manage Results page. There, users may generate a list of incidents, or a list of controls in which each control links to a list of the incidents it has generated.

Each of these incidents defaults to an Assigned status. This means that the result investigator is assigned to address the incidents generated by a control. The investigator might:

- Look at the incidents generated by a control, decide that nothing need be done to resolve them, and change status to Accepted.
- Look at the incidents generated by a control, decide that something must be done in the business-management application to resolve them, and change status to Remediation. For an AACG incident, a remedial action might be to rescind a user’s role assignment; or, it might involve excluding a privilege from the role through which a user has access to it.
- Ensure that appropriate action has been taken in the business-management application for an incident at the Remediation status, and update that status to Resolved.

For AACG detective analysis, the enforcement type assigned to the control — Prevent, Monitor, or Approval Required — serves as a guideline for what the result investigator may do (or recommend doing) in the business-management application. However, he can actually do whatever he determines to be necessary. For example, he may discontinue the access represented by one incident generated by a Prevent control, allow the access represented by another, and so eliminate the conflict while allowing some access. Moreover, a Simulation feature enables AACG users to forecast the impact of incident resolution on the business-management application.

When users are assigned duties after controls have been created to define them as conflicting, AACG may implement preventive analysis. In this case, a control’s enforcement type directly determines what happens:

- For a Prevent control, roles are denied to users if they lead to access points the control defines as conflicting. No incidents are generated, and there is nothing for the result investigator to do.
- For a Monitor control, roles are granted to users even if they lead to access points the control defines as conflicting. The next time the control is analyzed, the incidents resulting from the role assignments appear in the Manage Results page, and their status is Assigned. The result investigator may then update status; if so, the detective-analysis rules apply.
- For an Approval Required control, roles assigned to users are suspended until result investigators can review the assignments. If the control finds conflicts in Oracle Fusion, the review process is handled by Oracle Identity Management, not AACG. If the control finds conflicts in E-Business Suite or PeopleSoft, AACG handles the review process: Users, the roles assigned to them, and incidents generated by the control appear in a Manage Access Approvals page. There, a result investigator may approve or reject each role assigned to each user.

Regardless of where the conflict exists, when a role is approved and the control is subsequently analyzed, the related incidents appear in the Manage Incidents page, with the status set to Authorized. When a role is rejected, no records of related incidents appear in the Manage Incidents page. In either case, the result investigator need do nothing further.

In addition to the Assigned, Accepted, Remediation, Resolved, and Authorized statuses, AACG may automatically assign two other statuses to incidents. A Control Inactive status means that an incident is no longer of concern because the control that generated it has been inactivated. A Closed status indicates that because an incident has been resolved in the business-management application, a subsequent evaluation of controls finds that the incident need no longer be addressed.

(Each incident has not only status, but also one of three states: In Investigation, Approved, or Closed. These are assigned by GRC. See “Resolving Incidents,” page 4-1.)

Reporting

Users can run reports concerning AACG, its companion applications, and GRC administration. Those that apply to AACG include summary and detail reports about access controls, the incidents they identify, and the approval or rejection of role assignments that are subject to AACG preventive analysis.

Some reports can be run “contextually” — from pages in which controls are managed or incidents are resolved. Contextual reporting is discussed on pages 3-6 and 4-7.

All reports can be run from Report Management pages. Because Report Management features are common to all GRC applications, they are discussed in the *Enterprise Governance, Risk and Compliance User Guide*.

Common Procedures

As you work with AACG models, controls, and incidents, you may perform certain procedures that are common to GRC applications. You may use a home page or overview pages to view worklists (records of tasks requiring action on your part) and notifications (records of tasks in which you have an interest, but which do not require you to act). You may use navigation features to move among GRC application pages. You may use search features to filter lists of records. You may set “user preferences” — review and edit information about your user account. For complete information on these features, see the *Enterprise Governance, Risk and Compliance User Guide*.

Descriptions of other common procedures follow.

Selecting Perspectives

You can assign perspective values to models, continuous controls, and incidents generated by controls. These may serve as filtering values in the management pages for these objects, or in reports. They also play a part in determining which users have access to any of these objects — those whose job roles contain data roles associated with perspective values that match the values selected for the object. (Users must also have duty roles granting privileges to work with the object.)

Although perspective hierarchies are created in Perspective Management, each hierarchy becomes available for use with models, controls, or incidents only after being associated with that type of object in Manage Module Perspectives. In the pages for creating, editing, or resolving these objects, a Perspective Assignment panel displays a tab for each perspective hierarchy that has been associated with the object.

In Manage Module Perspectives, a perspective may be designated as required for the object with which it is being associated. If so, the tab that displays its name also displays an asterisk; a user is unable to save an instance of the object if he does not select a value for the required perspective.

When you create or edit models, create controls or edit them individually, or edit incidents individually, you select a set of perspective values for the object with which you are working. When you “mass edit” controls or reassign a set of incidents, you select perspective values to be added to, or removed from, the values already selected for each of the objects with which you are working.

To select perspective values:

1. Click on the tab for the perspective hierarchy from which you want to select values.
2. If you are editing two or more selected controls at once, or assigning two or more selected incidents simultaneously, select an Add or Remove radio button to indicate whether you are adding values to, or removing them from, values already selected for the objects with which you are working. (If you are creating objects or editing them individually, this step does not apply, and the radio buttons do not appear.)
3. Choose values to move between Available Perspectives and Selected Perspectives lists. (Ultimately, those in the Selected Perspectives list are assigned to individually configured objects, or added to or removed from those already assigned to mass-edited objects.) In either list, locate a perspective value you want to move from one list to the other. Do any of the following:
 - Click on the plus sign next to the root node to expose perspective values at the next hierarchical level. Click on a plus sign next to a node at that level to reveal its child nodes. Continue until you reach the node you want.
 - Type a text string in the search box to produce a list of matching perspective-value names. You can use the percent sign (%) as a wild-card character; entries are not case-sensitive. A search returns only matching perspective values; it does not display an entire perspective hierarchy.
 - For incidents only, select View > Expand All to display, and choose from, all nodes configured for the perspective. Other View options enable you to collapse the entire hierarchy, expand or collapse nodes beneath a selected node, display only a selected node and those that descend from it, and scroll to the first or last node.

If you are assigning perspective values to models or controls, you can choose them only one at a time; click on the value you want. If you are assigning perspective values to incidents, you may choose one value by clicking on it; choose a continuous set by clicking on the first, holding down the Shift key, and clicking on the last; or choose a discontinuous set by holding down the Ctrl key as you click on values.

4. Click the > button to cause values chosen in the Available list to appear in the Selected list. Or, click the < button to remove values chosen in the Selected list from that list.

(Alternatively, click the >> button to place all perspective values in the Selected list, or the << button to remove all values from that list.)

5. Repeat steps 1–4 to select any number of perspective values from any number of hierarchies.

As you assign perspective values to incidents, you may also select a View Perspective button to see a representation of the full hierarchy from which you are selecting a value. Click on any value, and a Related Components panel opens, displaying objects with which the value is associated. (This feature is not available as you assign perspective values to models or controls.)

Synchronizing Data

Models and controls evaluate access granted in datasources (instances of business-management applications). It's assumed that a set of datasources is configured for your AACG instance. (See the *Enterprise Governance, Risk and Compliance User Guide*.)

For models and controls to recognize changes made in their datasources, you must synchronize data — run a process that captures changes made since the last time a model or control was run. To complete this process:

1. Open a Manage Application Datasources page: select Setup and Administration under Tools in the Navigator, then Manage Application Datasources under Setup.
2. Select the row for the datasource with which you want to synchronize data.
3. Do either of the following:
 - Click on Actions > Synchronize Access. This causes data used by AACG to be synchronized once, immediately.
 - Click on Actions > Schedule Synchronize. A Schedule Parameter dialog opens; in it, you may create a schedule on which any number of synchronization operations run automatically. Select the Access check box to synchronize data used by AACG, and enter values that set the name of the schedule, its start date and time, the regularity with which the synchronization should occur, and an end date (if any). Then click on the Schedule button.

Each data synchronization job is incremental. Rather than reload all ERP data, the synchronization job updates data existing from the last job, editing existing records or adding new records as needed.

Attaching Files

In the pages in which you create or edit incidents, you can attach files to them. An attachment may, for example, be a text file, spreadsheet, or web site that provides more information about an object than can be contained in its Description field.

For most attachments, you need to specify a content type. These values are configured in Manage Content Types, which is available in the Setup and Administration

tasks. If no existing content type is appropriate for your attachment, have one created in Manage Content Types. (See the *Enterprise Governance, Risk and Compliance User Guide*.)

To attach a file:

1. Click on the green plus sign next to the Attachment label in a create or edit page. An Attachments pop-up opens.
2. Select Actions > Add. A new row appears.
3. Select a Type — desktop file or url. (During a mass update of incidents, only a url can be attached.)
4. 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.)
5. If you wish to create additional attachments, repeat steps 2 through 4 for each attachment.
6. Click the OK button to exist the Attachments pop-up.

You can also delete an attachment by opening the Attachments pop-up, selecting a row, and selecting Actions > Delete.

To view an attachment, click on its name in the management, creation, or edit page for an object.

Importing and Exporting CCM Elements

You can export CCM elements from a source instance to a file, or import them from a file to a destination instance. These elements include models, controls, and global conditions (which set limits on conflicts identified by models and controls).

However, several rules apply:

- “Seeded content” is a set of models (but not controls or global conditions) developed by Oracle for use with GRC. A version of seeded content is released with each GA release of GRC. That version of seeded content can be imported into the GA release or any patch to that release.
- Models, controls, or global conditions exported from an instance of a GA release can be imported into any patch for that release (but not from one patch to another, or one GA release to another).
- Models, controls, or global conditions exported from a GRC instance at any particular version can be imported into another instance at the same version.

To export models, controls, or global conditions:

1. In the Manage page for models, controls, or global conditions, select items to export. 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 the Ctrl key as you click on items.

2. Click on Actions > Export. 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. In the Manage Jobs page, locate the row displaying the job ID you noted in step 2. In its Message cell, click on the Job Completed link.
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. The file is saved in .xml format. The first word of its name —*Models*, *Conditions*, or *Controls* — identifies its content.
6. Close the Job Detail window (click on its OK button).

Models and controls may specify perspective values, and upon import are available to users whose data roles are associated with those perspective values. (Before importing, be sure the perspectives are set up in the target instance.) Global conditions do not specify perspective values.

To import:

1. Return to the Manage page for the item you are importing — models, global conditions, or controls.
2. Click on Actions > Import.
3. An Import File pop-up window opens. Click on its Browse button.
4. A Choose File dialog opens. In it, navigate to, and select, the .xml 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. Click on the OK button in the Import File window.
6. A Select Items to Import window lists the items contained in the import file. Select those you wish to import, bearing in mind that you can import only those items that use business objects to which your GRC roles grant you access. To select one item, click on it. To select a continuous set, click on the first item, hold down the Shift key, and click on the last. To select a discontinuous set, hold down the Ctrl key as you click on items.
7. Click on the Next button. An Import Datasource Mapping window opens, displaying one row for each datasource specified in the items you've chosen to import. For each, in a Mapped Datasources list box, select a datasource appropriate for the environment into which you are importing the models. (The list box displays datasources configured in the GRC Manage Application Datasources page, to which your GRC roles provide you access.)
8. Click on the Import button. A pop-up message reports the number of items imported and the status of the import operation. Click on its × button to close it.

Creating and Managing Models

An access model specifies access points (duties) in business applications that, in combination, enable individual users to complete risky transactions. A model consists of filters, which may serve either of two purposes:

- A filter may specify an access point or an entitlement (a set of access points); if so, it identifies users who have been assigned the specified access point, or any access point in the specified entitlement. A conflict exists when a user is selected by a combination of these filters. Combinations are determined by the way you arrange filters in the model.

In Oracle E-Business Suite, access points include roles, responsibilities, menus, functions, grants, and concurrent programs. In PeopleSoft, they include roles, permission lists, panel group components, menus, and page definitions. In Oracle Fusion, they include roles, privileges, and permissions. (AACG can recognize access points in Fusion only if a “connector” for Fusion Applications is installed.) For any of these applications, you can create user defined access points (see page 2-15), each of which is a specific path leading to a seeded access point — for example, a PeopleSoft page reached from one menu, but not from another.

- A filter may define a condition, which sets limits on the conflicts a model may identify. Typically, a condition specifies users or other items (such as companies in PeopleSoft or operating units in Oracle EBS) that are excluded from analysis by the model, or it specifies a type of item (operating unit, for example) and requires that the model return results only when access points conflict within individual instances of that item type.

A global condition, which applies to all models that run in a given datasource, also uses filters, which are exactly like those that define model-specific conditions.

AACG provides pages for creating access models and global conditions, and for managing them once they are created. It also provides capability to create entitlements and another type of condition — a “path condition.”

Managing Models

A Manage Models page provides information about access or transaction models to which your data roles give you access. (Transaction models are created in Enterprise Transaction Controls Governor, or ETCG.) Within that limitation, you can view and work with models created by any user — create or modify models, view or export

results, visualize access results, or export and import models (page 1-7). To open the page, select Manage Access Models from among the Continuous Control Management tasks available from the Navigator.

Viewing Models

In the Manage Models page, a “My Models” panel displays a list of access models if you select Manage Access Models in the Tasks list, or of transaction models if you select Manage Transaction Models.

The page displays summary information for each model it lists. This information is supplied by GRC, from data recorded when a model is created, edited, or run; you cannot update these records directly.

Among the summary values, the model type is Access, Transaction—Defined, or Transaction —Pattern. An Access model defines conflicts among access points in a company’s systems. The other types evaluate transaction risk. (For more on transaction models, see the *Enterprise Transaction Controls Governor User Guide*.)

Model status indicates whether the model has been evaluated and has produced results — records of access it has found to be risky. Values include Not Started, Started, Completed, and Canceled. In addition, an Error status links to the GRC Jobs page, which can provide information about processing errors. Model state is either Approved or Invalid (the latter state applying only to models that are not imported correctly during an upgrade from an earlier version).

Creating, Editing, Copying, or Deleting Models

To create an access model, select a Create Access Model option, which is available both in the Actions menu of the Manage Model page and among the Continuous Control Management tasks available from the Navigator. Either selection opens a Create Access Model page (see “Creating an Access Model,” page 2-3).

To edit an access model, click in the My Models panel on the row for the access model you want to edit. Then click on Actions > Edit. This opens an Edit Access Model page— a replica of a model-creation page, except that it is populated by values for the model you want to edit.

Rather than create a model from scratch, you can copy an existing model, then modify the copy. To do so, select (click on) the model you want to copy. Then select Actions > Copy. A new row appears in the My Models panel, identical to the listing for the copied model except that the model name ends in a number in parentheses. (The value of the number depends on how often you copy the original.) Once the copy exists, you can select Actions > Edit to modify the model as you please.

To delete a model, click in the My Models panel on the row for the model you want to delete. Then click on Actions > Delete, and respond to a pop-up message that asks you to confirm the deletion.

Model-Data Synchronization

The Actions menu of the Manage Model page includes a Synchronize option, but this option applies *only* to transaction models. To synchronize data used by access

models, do not use this option. Instead, follow the procedure described in “Synchronizing Data” on page 1-6.

Creating an Access Model

To create an access model:

1. Open the Create Access Model page: Click on Actions > Create Access Model in the Manage Model page (see page 2-2). Or, select Create Access Model among the Continuous Control Management tasks available from the Navigator.
2. Name and describe the model (below).
3. Select business objects (below) and datasources (page 2-5). These supply the access data the model will evaluate.
4. Create filters. As you create them, arrange their vertical and horizontal alignment to one another, to set the order in which they are to be evaluated (pages 2-6 through 2-11).
5. Optionally, select perspective values for the model (see page 1-4).

Each model is automatically assigned values for CCM Type, Business Object, and Datasource system perspectives. These values represent selections you make as you create the model — whether it is an access or transaction model, and the datasources and business objects you select for it. So at minimum, a model is restricted to users whose data roles include matching values for system perspectives. You can assign other perspective values, further restricting the model’s availability. Perspective values associated with a model also apply to any control developed from the model.

6. Save the model (page 2-11).

Naming the Model

Near the top of the Create Access Model page, locate the Name field. Click in it, and type a name for your model. Then click in the Description field immediately below the Name field, and enter a brief explanation of the purpose for the model.

Alongside the Name field, a Datasource field displays the datasources subject to the model you create. Initially, the field may be blank. You can add datasources to the model, or delete datasources, but you do so elsewhere. GRC updates the Datasource field, and you cannot do so directly.

Selecting Business Objects

A business object corresponds to one or more database tables (existing in one or more datasources) that hold information pertinent to user access. Select one or more:

- Add the Access Point business object to your model if you intend to create a filter that specifies an access point (and returns users who have been assigned that access point).

- Add the Access Entitlement business object to your model if you intend to create a filter that specifies an entitlement (and returns users who have been assigned any access point included in that entitlement).
- Select among four other business objects — EBS Access Condition, PeopleSoft Access Condition, Fusion Access Condition, and Page Access Configurations — if you intend to create a condition filter (which defines exemptions from analysis by a model).

A model may include a filter that selects users with access to a page, but to eliminate false positives, it may also include a condition that excludes those who are not authorized to perform particular actions in that page. The Page Access Configurations business object provides values for use in such condition filters. For the current release, this business object applies only to PeopleSoft, in which “user preferences” determine what users can do in pages to which they have access; the Page Access Configurations object consists of user-preference values. (For example, a model concerned with the creation of adjustment vouchers could include a filter that selects users with access to the Create Voucher page. It could also include a condition filter to exclude those who do not have the Allow Adjustment Voucher user preference, and therefore cannot actually create an adjustment voucher.)

Each of the remaining three condition business objects supports a type of data-source (EBS, PeopleSoft, or Fusion), and is available only if a datasource of its type has been set up and synchronized in the Manage Application Datasources page.

To add business objects to a model:

1. In a grid at the left of the Create Access Model page, select (click on) the Business Objects tab, and then on an object in the grid. (Although unlabeled, this grid is known as “the Library.”)
2. Do either of the following:
 - In the Library, click on the Add to Model button. The selected business object appears in the panel labeled “Model Objects.”
 - Use your mouse to drag the business object to the area labeled “Add Object Here” in the Model Objects panel.
3. Repeat this process if you wish to add more objects to the model.

Within the Model Objects panel, each object appears as a window that lists the attributes belonging to the object. In this window, you can view, but not actually select, the attributes. You can, however, do the following:

- Remove a business object from the model: click on its × button.
- Move a business object to the left or right of other objects: Click on the downward-pointing, green triangle. Two options appear; click on either Move Left or Move Right.
- Create custom attributes. (You can do so, however, only after having selected at least one datasource for the business object with which you’re working.)
 1. Click on the green + icon. An Add Custom Attribute dialog opens.
 2. In an Attribute Name field, create a name for the new attribute.

3. In a Base Attribute field, select one of the existing attributes.
4. In a Modifier field, select a mathematical operator: + (addition), – (subtraction), * (multiplication), / (division), or & (creates a comma-delimited text string of the combined values). You are able to select only among modifiers appropriate for the base attribute selected in step 3. For example, you can subtract dates, but you cannot multiply them.
5. In a Type field, select Value or Object.
6. If you selected Value, enter a value to be combined with the Base Attribute, as defined by the Modifier.

If you selected Object, select a second attribute, whose values are combined with those of the Base Attribute, as defined by the Modifier.
7. Click on the OK button.

You can use the custom attribute in filters. Custom attributes appear at the top of the list of attributes displayed by the business object, and each has an edit icon (which looks like a pencil). You can click on a custom attribute to open another dialog box in which you may either edit or delete the custom attribute.

Selecting Datasources

Before a business object can supply access points, entitlements, or other data to a model, it must be associated with at least one datasource. As the model is evaluated, a filter citing that business object will analyze data supplied by the associated datasource.

- Associate the Access Entitlements business object with a datasource called Grc — the AACG instance in which you are working, and have configured entitlements for use in models. (The Grc datasource exists automatically.)
- Associate any of the other four business objects — Access Point, EBS Access Condition, PeopleSoft Access Condition, and Fusion Access Condition — with datasources for instances of business-management applications in which a model is to be run. (These datasources are configured in the GRC Manage Application Datasources page.)

In the Manage Application Datasources page, one datasource may be designated as default. If so, that datasource is associated with any business object (other than Access Entitlements) as soon as you select it for a model. (No matter whether a default datasource has been configured, you must actively select the Grc datasource for the Access Entitlements business object.)

As you add business objects to a model, you can change, or add to, their default datasource selection. If no default datasource has been designated, you can add datasources to each business object. To do so:

1. When you add a business object to the Model Objects panel, a Manage Datasource button becomes active. Click on it. A Manage Datasource window opens.
2. To add a datasource, create a new row: click on Actions > Create New, or on the green + sign. (Multiple rows can exist for each business object.) To change a datasource selection already made for an object, work in its existing row.

3. If you're adding a datasource, click in the Business Object field of a new row and select the business object for which you want to add a source. If you're modifying an existing datasource, locate the row in which the Business Object field displays the name of the object whose source you want to change.
4. Click in the Datasource Name field. From its list of datasources, click on the datasource you want to associate with the business object. Other fields are populated automatically.
5. Click on the Save and Close button. If you've added datasources, their names appear in the Datasource field (alongside the Name field near the top of the Create Access Model page.)

You can also delete the association of a datasource with a business object. While the Manage Datasources window is open, select (click on) the row for the association you want to delete. Click on Actions > Delete or on the red × icon.

Arranging Filters

Each filter you create appears as a dialog box in a Model Logic panel. To define a filter, make selections in the fields displayed by its dialog box. As you add access point or entitlement filters, position each vertically or horizontally with respect to others:

- A vertical arrangement indicates an AND relationship: Filters at one level are evaluated before those at the level below it, the topmost first and the bottommost last. Presuming that processing at any vertical level returns records, processing continues on those records at the next level. For the model to return any results, every vertical level must evaluate to true.

For example, a model contains two filters, one above the other. The upper filter identifies users assigned one access point, and the lower identifies users assigned a second access point. A conflict exists for each user identified by both filters.

- A horizontal arrangement indicates an OR relationship: If any one filter within a horizontal set returns results, processing moves to the next vertical level.

For example, two filters alongside one another may be positioned above a third filter. Each filter specifies its own access point. A conflict would exist for each user assigned either of the first two access points, and the third access point.

The placement of condition filters is irrelevant. All condition filters are evaluated (regardless of whether they are placed vertically or horizontally to other filters, or before or after them), and each condition filter excludes conflicts from the set returned by access point and entitlement filters.

For example, suppose a model contains two filters, each of which identifies an access point. The filters are positioned one above the other, indicating that the access points conflict. Suppose the model also contains two condition filters: One selects a user to whom the model applies. The other identifies an operating unit for exclusion from processing. From the set of all conflicts involving the two access points, the model would exclude conflicts involving all users other than the one named in the first condition, and conflicts involving the operating unit named in the second condition. It would return only those conflicts that remain. It would do so regardless of where each condition filter is placed with regard to other filters.

To add filters to a model, click on the New Filter button (or a New Filter option in the Actions menu). As you do, keep these concepts in mind:

- When you add a filter, it appears by default immediately beneath the lowest filter in your model hierarchy. If, for example, a model contains four vertical levels and you click on the New Filter button, a filter appears at the fifth vertical level.
- You can drag and drop existing filters to new positions within the model. Move the mouse cursor to the upper middle of the filter you want to move. The mouse cursor turns into a four-pointed cross. Left-click, hold the mouse button down, and do either of the following:
 - To rearrange or create an AND (vertical) relationship, drag the filter to an arrowhead above or beneath any other filter. One exception: You cannot drag a filter above the first filter in your model hierarchy (although you can drag that first filter below any other).
 - To create an OR (horizontal) relationship, drag the filter on top of any other filter. (“On top of” means that you move one filter so that it takes up the same space as, and so obscures, another. It does not mean that you drag a filter to the upper border of another.) You can add any number of filters to the OR relationship by dragging each new filter on top of any filter currently in the OR relationship.
- Once two or more filters exist in your model, you can select them: hold down the Ctrl key and click in the title field (labeled *Filter*) of each filter you want to select. When you select a filter, the interior of its dialog box turns a dark shade. (An unselected dialog box is light blue.) You can select one or multiple filters, but in the latter case, select filters that are adjacent to one another.
- You can incorporate filters into groups: select those you want to include and click on the Group Filters button (or on Actions > Group Filters). You can drag and drop groups in the same ways as individual filters. To dissolve a group, select it and click the Ungroup Filter button (or Actions > Ungroup Filter). If you dissolve a group embedded in an OR relationship, the filters are moved to the position right after the relationship.

Create structures as complex as you like. For example, an OR statement may contain any number of filters.

Or, a filter may have an AND or OR relationship with blocks of other filters. For example, suppose filters One, Two, and Three are in an AND relationship — stacked vertically. You could drag Three into a horizontal pairing with Two; One would remain centered above them. If each filter named an access point, the model would identify users assigned access point One and either access point Two or Three.

For another example, suppose filters One, Two, Three, and Four are stacked vertically. You can select One and Two and enclose them in a group, select Three and Four and enclose them in a group, and then drag the Three and Four group into a horizontal pairing with the One and Two group. If each filter named an access point, the model would identify users assigned either access points One and Two, or access points Three and Four.

Creating an Access Point or Entitlement Filter

To create an access point filter (one that specifies an access point, and returns users who have been assigned that access point) or an entitlement filter (one that specifies an entitlement, and returns users who have been assigned any access point included in that entitlement):

1. Click on the New Filter button, or on Actions > New Filter. A dialog box appears in the Model Logic panel.
2. Enter a name for the filter in the Filter field.
3. An Object field lists the business objects you've added to the model in the Model Objects panel. Select (click on) Access Point for an access point filter, or Access Entitlement for an entitlement filter.
4. Accept default values in an Attribute field (Access Point Name for an access point filter, or Access Entitlement Name for an entitlement filter) and a Condition field (Equals in either case).
5. To the right of a Value field, click on an icon that looks like a magnifying glass. A pop-up window opens, in which you will ultimately select an access point (for an access point filter) or an entitlement (for an entitlement filter). The filter will return users who have been assigned the access point you select, or any access point in the entitlement you select.
6. Use filtering tools to search for the access point (seeded or user defined) or entitlement you want to select. Enter complementary values in any combination of the following four fields. In each, you can use the percent sign (%) as a wild-card character to search for a selection of values that contain a text string.
 - Name: Type a text string to search for matching display names of access points or entitlements.
 - Description: Type a text string to search for matching internal names of access points, or descriptions configured for entitlements.
 - Datasource: Enter a datasource name for a business-application instance whose access points you want to use. For each entitlement, the field displays datasources — potentially multiple — for access points included within the entitlement.
 - Type: If you are searching among access points, select a type. Valid values include Function, Responsibility, Role, Menu, Grant, and Concurrent Program in an Oracle EBS context; Permission List, Panel Group Component, Menu, Role, and Page Definition in a PeopleSoft context; Role, Privilege, and Permission in a Fusion context; and User Defined in any of these contexts. If you are searching among entitlements, the only valid value is Entitlement.
7. Click on the View button. The Access Point List window then displays access points or entitlements that match your filtering criteria.
8. Click on the access point or entitlement you want to select, and then on the OK button. The pop-up window closes, and your selection populates the Value field of the filter.

Creating a Condition Filter

To create a filter that defines an access condition:

1. Click on the New Filter button, or on Actions > New Filter. A dialog box appears in the Model Logic panel.
2. Enter a name for the filter in the Filter field.
3. An Object field lists the business objects you've added to the model in the Model Objects panel. Select (click on) one from which you want to choose an attribute for use in this filter — EBS Access Condition, PeopleSoft Access Condition, Fusion Access Condition, or .
4. In the Attribute field, select an attribute on which you want to base a condition.
 - To create a condition that excludes an item from analysis by the model, select its type as an attribute — for example, Set of Books in the EBS Access Condition business object. (If you're basing the condition filter on the Page Access Configurations object, Page Access Configuration Name is the only attribute you can select.)
 - To create a condition that requires the model to find conflicts for access points assigned only within instances of an item type, select one of the "Within Same" attributes — for example, the Within Same Set of Books attribute in the EBS Access Condition business object.
5. A Condition field presents a list of operators that may be applied to the attribute you selected, usually to force a comparison between each attribute value and a third (yet-to-be specified) term in the filter. Select one. The following operators are available for attributes that are not dates, although you will see only those appropriate for the attribute you've selected:
 - Equals and Does not equal: The filter returns results if the value of the attribute matches or does not match a specified value. If you selected a "Within Same" attribute in step 4, Equals is the only operator available to you.
 - Contains and Does not contain: The filter returns results if the value of the attribute is a text string that includes, or excludes, a specified text string.
 - In and Not in: The filter returns results if the value of the attribute is a text string that matches, or does not match, a value in a semicolon-delimited set of text-string values. The match must be exact.

In addition to Equals and Does not equal, the following operators are available for date attributes:

 - Mathematical operators: The filter returns results if the value of the attribute is less than, less than or equal to, greater than, or greater than or equal to a specified date.
 - Between: The filter returns results if the value of the attribute falls between two other specified dates.
 - Is blank and Is not blank: The filter returns records for which the attribute column either contains no date, or contains any date.
6. Define the third term of the filter. You have several options, which depend on selections you made in steps 4 and 5.

First, if you selected a “Within Same” attribute in step 4, a Type field defaults to Value. In a Value field, select Yes to find conflicts for access points assigned within, but not across, instances of the item you specified in step 4.

Second, if you selected a date attribute in step 4, and the Is Blank or Is Not Blank operator in step 5, you need do nothing further. If you selected any other operator in step 5, select Fixed Value or Relative Value in a Type field.

- If you select Fixed Value, a Value field appears. Click in that field or on an icon next to it. A pop-up window displays a calendar; in it, select a date.
- If you select Relative Value, Value and Units fields appear; in them, specify a number of days, weeks, or months from the system date.

Third, if you selected an attribute in step 4 that is neither a date nor one of the “Within Same” attributes, make a selection in a Value field:

- a** Click on an icon that looks like a magnifying glass. An Attribute Values List pop-up window opens. It lists values that correspond to the attribute you selected in step 4 — for example, sets of books if you selected the Set of Books attribute from the EBS Access Condition business object, or names of user preferences from the Page Access Configurations business object.
 - b** Use filtering tools to search for a value you want to select — for example, a specific set of books or a particular user preference. Enter complementary values in any combination of the following three fields. In each, you can use the percent sign (%) as a wild-card character to search for a selection of values that contain a text string.
 - Name: Type a text string to search for matching internal names.
 - Display Name: Type a text string to search for matching display names.
 - Datasource: Enter a datasource name for a business-management-application instance whose data you want to use.
 - c** Once you have entered filtering values, click on the View button. The Attribute Values List window then displays values that match your filtering criteria.
 - d** Click on the value you want to select, and then on the OK button. The Attribute Values List window closes, and your selection populates the Value field of the filter.
7. If appropriate, click on the ± toggle next to an Advanced Options label, then select the Exclude advanced option. This removes records defined by the filter from analysis; in effect the filter returns all records that do not meet its specifications.

For example, if you selected the Set of Books option from the EBS Access Condition business object in step 4, Equals in step 5, the name of a specific set of books in step 6, and the Exclude option in step 7, that set of books would be removed from analysis by the model.

For another example, suppose you selected Page Access Configuration Name from the Page Access Configurations business object in step 4, the In operator in step 5, and the Allow Adjustment Voucher and Allow Claim Voucher names in step 6, and you left the Exclude check box unselected. If the model also contained a filter that

returned users with access to the Create Voucher page, the model would select only those who also have one of those two voucher styles (and exclude everyone else).

Note: If conditions that cite the Page Access Configurations business object do not effect exclusions as you expect, ensure that users actually have the user preferences you mean to exclude. PeopleSoft appears to select default user preferences for users, but these are actually suggested values; they are not active for a user unless they are saved for that user in PeopleSoft.

There may be more than one way to configure a given condition. For example, to exclude a set of books called “SOB1,” you might create a filter in which the Set of Books attribute from the EBS Access Condition business object equals SOB1, and then select the Exclude advanced option. But this would effectively be the same as choosing the Set of Books attribute from the EBS Access Condition object, Does not equal, and SOB1, and clearing the Exclude advanced option.

Saving the Model

To save the model, click on the Save button or the Save and Close button. Both are located near the upper right corner of the Create Access Model page. The Save option saves the model, but leaves its values on display for potential further editing, or for the generation of results. The Save and Close option saves the model but empties the Create Access Model page so that it is ready for the creation of a new model. Alternatively, you can click the Cancel button and respond to a confirmation prompt to restore the blank Create Access Model page without saving the model.

Managing and Creating Global Conditions

A global condition sets limits on the conflicts identified by all access models or controls evaluated on a given datasource. Like a condition written for a specific model, a global condition typically specifies users or other items (such as companies in PeopleSoft or operating units in Oracle EBS) that are excluded from analysis by a model or control, or it specifies a type of item (operating unit, for example) and requires the model or control to return results only when access points conflict within individual instances of that item type.

A Manage Access Global Conditions page lists these global conditions, displaying summary information about them: name and description, status (Active or Inactive), and datasource. To open this page, select Manage Access Global Conditions among the Continuous Control Management tasks available from the Navigator. The values it displays are updated by AACG, from information recorded when a condition is created or edited; you cannot update them directly.

Creating Global Conditions

The process of creating a global condition is essentially like creating an access model that contains only condition filters. As you create filters for a global condition, however, AACG places them horizontally to one another, indicating an OR relationship — the condition produces results if any (or any combination) of its filters evaluates to true. You cannot arrange condition filters to create AND relationships. Moreover, each global condition applies to a single datasource.

To create a global condition:

1. Click on Actions > Create New in the Manage Access Global Conditions page. Or, click on Create Access Global Condition from the Continuous Control Management tasks. Either action opens a Create Access Global Condition page.
2. Near the top of the Create Access Global Condition page, locate the Name field. Click in it, and type a name for your global condition. Then click in the Description field immediately below the Name field, and enter a brief explanation of its purpose. Finally, in the Status field, select a status for the condition — typically Active. (You cannot delete a global condition; you can only inactivate it.)
3. Select the EBS Access Condition, PeopleSoft Access Condition, or Fusion Access Condition business object, depending on whether you want the global condition to apply to an Oracle EBS, PeopleSoft, or Fusion instance.

The procedure for doing so is the same as for models (see “Selecting Business Objects” on page 2-3), except that (here and in following steps) labels in the Create Access Global Condition page apply to conditions. (Here, for example, an Add to Condition button replaces the Add to Model button, and a Condition Objects panel replaces the Model Objects panel.)

4. Select a datasource to which the condition will apply. The procedure for doing so is the same as for models (see “Selecting Datasources” on page 2-5), except that you can select only one datasource for the global condition.
5. Create one or more filters. The procedure for doing so is the same as the one for creating condition filters for an access model (see “Creating a Condition Filter” on page 2-9).
6. Save the global condition: Click on the Save button or the Save and Close button. Both buttons are located near the upper right corner of the Create Access Global Condition page. The Save option saves the condition, but leaves its values on display for potential further editing. The Save and Close option saves the condition but empties the Create Access Global Condition page so that it is ready for the creation of a new condition. Alternatively, you can click the Cancel button and respond to a confirmation prompt to restore the blank Create Access Global Condition page without saving the model.

Editing or Copying Global Conditions

To edit a global condition, click in the Manage Global Access Conditions page on the row for the condition you want to edit. Then click on Actions > Edit. This opens an Edit Access Global Condition page — a replica of a condition-creation page, except that it is populated by values for the condition you want to edit. Modify values as described in “Creating Global Conditions” (page 2-11).

Rather than create a condition from scratch, you can copy an existing condition, then modify the copy. To do so, click in the Manage Global Access Conditions page on the row for the condition you want to copy. Then select Actions > Duplicate. A new row appears in the Manage Global Access Conditions page; it’s identical to the listing for the copied condition except that the condition name ends in a number in parentheses. (The value of the number depends on how often you copy the original.) Once the copy exists, you can select Actions > Edit to modify it as you please.

Managing and Creating Entitlements

An entitlement is a set of related access points. Within an access model or control, a filter that specifies an entitlement identifies users who have been assigned any access point in the entitlement. To work with entitlements, select Manage Access Entitlements among the Continuous Control Management tasks available from the Navigator.

Creating an Entitlement

To create an entitlement:

1. In the Manage Access Entitlements page, click on Actions > Add. A new row appears in the grid, second from the top.
2. Insert the following values in the new row. To do so, double-click in each field, or press the Tab key to move from an active field to the next field.
 - Entitlement Name: Type a name for the new entitlement.
 - Description: Explain briefly the organizing principle or business purpose of the entitlement.
 - Comments: Record additional statements about any aspect of the entitlement.
 - Status: Select Active or Inactive. (An Inactive entitlement cannot be selected for use in an access model or control.)
 - Effective Date: Select a date on which AACG can begin to use the entitlement. (Its status must also be set to Active.) Either accept the default value — the current date — or double-click in the Effective Date column, and then click on the grid-like icon it presents. A pop-up calendar appears. In it, click on the left- or right-pointing symbol surrounding the month and year to display an earlier or later month. Or, click on the downward-pointing symbol to produce a list of months in the current year, and click on the one you want. Then, in the calendar, click on the date you want. Alternatively, click on the Today button to select the current date.

Adding Access Points to an Entitlement

To add access points to an entitlement:

1. In the upper grid, select the row for the entitlement to which you want to add access points. (If you are creating a new entitlement, the row is necessarily already selected. If you are editing an existing entitlement, double-click on the row.)
2. Click on the Access Points button in the bottom portion of the Manage Access Entitlements page. A pop-up window, titled Access Point List, appears.
3. Use filtering tools to generate a list of access points (seeded or user defined) from which you can select as you build your entitlement. You can use the percent sign as a wild-card character, and you can enter complementary filtering values in any combination of the following fields:
 - Operand Name: Type a text string to search for matching display names of access points.
 - Description: Type a text string to search for matching internal names of access points.

- Datasource: Enter a datasource name for a business-application instance whose access points you want to use. An access point is specific to the instance in which it runs. If, for example, an organization runs two Oracle EBS instances, each function, responsibility, or other access point would be available for selection twice, once for each instance. Use this filter to ensure your entitlement contains access points selected from the instance you want.
 - Platform: Enter a business-management-application type — such as Oracle or PeopleSoft — whose access points you want to use. (These values are set during data-source configuration.)
 - Operand Type: Select a type of access point for which you wish to search. Valid values include Function, Responsibility, Role, Menu, Grant, and Concurrent Program in an Oracle EBS context; Permission List, Panel Group Component, Menu, Role, and Page Definition in a PeopleSoft context; Role, Privilege, and Permission in a Fusion context; and User Defined in any of these contexts.
4. Once you have entered filtering values, click on the View button. The search window then displays access points that match your filtering criteria.
 5. Select access points to add to the entitlement, and drag them into the Entitlement Details area of the Manage Access Entitlements page. To select a single access point, 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 access points.
 6. If you need to select additional access points that were excluded by your original filtering criteria, click on the Clear View button in the search window, enter new filtering criteria, and drag additional items into the Entitlement Details area of the Manage Access Entitlements page. When you finish selecting access points, close the search window by clicking on the × symbol in its upper right corner. The Entitlement Details area now lists the access points you selected.
 7. For each access point, confirm that the status column reads “Active.” (This should be the default.) If you wish to inactivate any access point, double-click in its cell in the Status column; this activates a list box, in it, select Inactive. Typically, however, you want the access points you’ve selected to be active, and so would leave the Status settings as they are.

The Change Control and Audit check boxes are reserved for future development, and have no meaning. The Access Control check box is selected because the access point is available for use in access controls. Other columns display values as described in step 3, with “Element Name” corresponding to “Operand Name” and “Element Type” corresponding to “Operand Type.”

8. When you are done, click Actions > Save button . A message indicates that the entitlement has been saved; click on its OK button to clear it.

Editing an Entitlement

You can edit an entitlement, essentially by selecting its row in the upper grid of the Manage Access Entitlements page and following the processes described in “Creating an Entitlement” (page 2-13) and “Adding Access Points to an Entitlement” (page 2-13). You can alter any aspect of the entitlement — not only the values set in

the fields of the upper grid, but also the selection of access points. Add access points as you would to a new entitlement. To remove an access point, you have two options:

- Inactivate it: Click on its cell in the Status column in the bottom portion of the Entitlements page. In the list, select the Inactive value.
- Delete it: In the bottom portion of the Entitlements page, click on the row for the access point, and then click on the Delete button

Use caution — if you edit an entitlement after it has been selected for use in a model or control, you necessarily alter the meaning of that model or control, potentially to the point at which it no longer defines meaningful conflicts.

When you finish making changes to the entitlement, click on Actions > Save to save your changes.

Copying an Entitlement

You can copy an entitlement as a template for the creation of a new entitlement:

1. In the upper grid of the Manage Access Entitlements page, click on the row for the entitlement you want to copy.
2. Click on Actions > Copy.

The copy is identical to the original, but inactive. (That is, the status field for the entitlement as a whole, located in the upper grid, is set to Inactive. The status for each member of the copied entitlement is set in the same way as it was in the original.)

After you make the copy:

- Use the procedures described in “Editing an Entitlement” (page 2-14) to modify its selection of access points as desired.
- Give the copy a new name that reflects the alterations you’ve made to it.
- When you are ready to use the entitlement, change its status to Active.
- Click the Save button to save your changes.

Managing and Creating User Defined Access Points

Whether an access point legitimately constitutes an element of an SOD conflict may depend on how the user can reach it. In PeopleSoft, for example, the Journal Entry page enables users both to enter and approve journals, so it may present a risk if a user can reach it through menus (or other components) that grant write access. However, it would not present a risk if a user reaches it through another path that provides only read access.

Thus, rather than include an access point in an access model or control, you may wish to include an access path. To this end, you can create a user defined access point (UDAP), which defines a specific path to a seeded access point.

For PeopleSoft analysis, a UDAP may incorporate user preferences (properties of individual users that determine what they may do in a given page). For example, a UDAP may specify a path to the Journal Entry page, but include in that path the “Journals: Approve” user preference. (It’s recommended that such a UDAP position

the user-preference value last in the path, for consistency as GRC displays paths in model results and control incidents.)

To create a UDAP, use the Manage Access Entitlements page. You may, in fact, create it as an independent item, or as one of the access points included in an entitlement. Either way, the process is similar to the process of creating an entitlement.

To create a user defined access point:

1. Create an entitlement (see page 2-13), or open an existing one.
2. In the bottom portion of the Entitlement page, click the Create Access Point button. A popup window, titled Access Point List, appears.
3. As you would for an entitlement (see steps 3 and 4 of “Adding Access Points to an Entitlement,” page 2-13), use filtering tools to generate a list of access points from which to select as you define a path for your UDAP.
4. Select access points and drag them into the open space at the bottom of the Access Point List window. All access points must come from a single datasource, each access point can be selected only once, and (in a PeopleSoft context) no more than one user preference can be selected.
5. Ensure that the access points are listed in the order that correctly defines the path you want to create. (The path begins with the access point at the top and ends with the access point at the bottom.) If not, rearrange them: Select each access point (as necessary) and use the Move Up and Move Down options of the Actions menu to change its position. (You can also delete an access point if it proves to be unnecessary; click on it and select Actions > Delete.)
6. Click the Save and Close button.
7. So far the UDAP is saved as an independent object. To include it as a member of the entitlement in which it was created, save the entitlement. Select Actions > Save in the upper portion of the entitlements page.

Once created, the UDAP is listed in the Access Point List popup window that you would use as you create either an entitlement or an access-point filter in an access model. Its name is the path that you created. In model results and control incidents, fields that report access-point names would also display the path that defines a UDAP.

You can delete a UDAP, although you must first remove it from any entitlement or model in which it is used. (You cannot delete it if it is used in a control.) To delete a UDAP, open the Manage Access Entitlements page, select any entitlement, and click the Access Points button. In the Access Points List window, search for and select the UDAP you want to delete. Then select the Delete option (in the menu bar of the Access Points List window, or its Actions menu). The Delete option is active only when a UDAP is selected.

Using Path Conditions

A path condition excludes one access point from another, such as an Oracle function from a menu or a responsibility. A path including those points would be excluded from incident generation. For example, an access control might set functions f1 and f2 in conflict. If a path condition excludes f1 from responsibility r1, and a user has

access to both functions, then no incident would be generated if the user's access to f1 comes from r1.

To create a path condition:

1. Select Manage Access Path Conditions, among the Continuous Control Management tasks available in the Navigator.
2. In the Datasource list box at the upper left of the Manage Access Path Conditions page, click on the datasource for which you want to configure path conditions.
3. Click on Actions > Add. A new row appears in the top section of the page. Its Instance field is set automatically to the datasource you selected in step 2, and the Action field to Exclude. These cannot be changed.
4. Double-click on each of the remaining fields. In each, a pop-up window presents a list; in it, select an appropriate value:
 - In the Access Point Type field, choose the type of access point you want to exclude from another.
 - In the Access Point field, select the specific access point to be excluded.
 - In the From Access Point Type field, select the type of access point from which you want to exclude the one you've already selected.
 - In the From Access Point field, select the specific access point from which the first is to be excluded.
 - In the Status field, accept the default value, Active, to use the condition, or select Inactive to hold it in reserve.
 - In the Comments field, briefly describe the purpose of the condition.
5. Click on Actions > Save.
6. Repeat these steps to create as many additional conditions as you wish.

To edit a path condition, select its row in the upper portion of the Manage Access Path Conditions page, and then select Actions > Edit. Select new values and then select Actions > Save.

To view the history of changes to path conditions, click on the row for a condition in the upper portion of the page. Change history appears in the lower portion — one row displaying the settings for each version of the condition up to, but not including, the current version.

Viewing or Exporting Model Results

From either the Manage Models page or the page in which you create or edit a model, you can view results from the most recent run of a model (if it has been run before), or run the model and view a new set of results.

Before running a model, consider synchronizing data from the datasource against which the model will run; this would ensure that access data is up to date. See “Synchronizing Data” on page 1-6.

No matter which page you use to display model results, a Results pop-up window presents a grid. Each row in the grid documents a path through which a user of a

business application, assigned access points that a model defines as conflicting, can reach one of those access points. The row also displays related information, such as the user's identity and the datasource on which the conflict exists.

To open the results window from the page in which you create or edit a model, select one of three buttons, which appear in the title bar of the Model Logic panel:

- **Run:** The model runs, and the page remains open. If the model had been run before, the new run overwrites the existing results (with no prompt to save or view them).
- **Run in Background:** The model runs, but you may navigate to another GRC page and work there. Again, if the model had been run before, the new run overwrites the existing results.
- **View Existing Results:** For a model that had been run before, the results window displays the results generated in the most recent run.

To open the results window from the Manage Model page, do either of the following:

- Locate the column labeled "View Results." In it, the entry for each model contains a prompt (which also reads "View Results") if the model has been run. (If not, the View Results cell is blank.) Click on the prompt (if one appears) for the model whose results you want to view.
- In the My Models panel, click on the row for the model whose results you want to view. Then, in the menu bar, select Actions > View Results.

If the model has not been evaluated previously, GRC simply runs it. If the model has been evaluated previously, a dialog box prompts you to decide whether to overwrite existing results. Select No to display the existing results. Select Yes to generate and display a new set of results.

To view the status of a model run, open a Manage CCM Jobs page: select Continuous Control Management under Continuous Monitoring in the GRC Navigator, then select Manage CCM Jobs under Control Administration in the Tasks list. For more on this feature, see "Jobs and Scheduling" in the *Enterprise Governance, Risk and Compliance User Guide*.

You can export model results to an Excel spreadsheet. To do so:

1. In the results window, click on Actions > Export to Excel.
2. A pop-up window offers you options to open or save the export file. Typically, click on its Save button and, in a Save As dialog, navigate to a folder in which you want to save the file.

Visualizing Access Results

As you view the results of access models (or incidents generated by access controls), you can generate a graphic depiction of paths from any number of users to any number of access points involved in conflicts.

1. In the Results window, select any number of paths. To select one, click on it; to select a continuous set of paths, click on the first one, hold down the Shift key, and click on the last one; or to select a discontinuous set of paths, hold down the Ctrl key as you click on the paths.

2. In the Results window, click on Actions > Visualize. A Graph window opens, depicting the paths you've selected.
3. Review information presented by the image:
 - The top-level node in a Visualization image is initially a user whose duty assignments have violated the access model. Depending on the paths you've selected in step 1, there may be more than one user.
 - The bottom-level nodes in a Visualization image represent the lowest-level objects affected by the model — those that actually enable a user to do something. For example, if a model sets one Oracle responsibility in conflict with another, the graph shows not only the responsibilities, but also the menus to which they lead and the functions to which those menus lead.
 - All nodes represent objects that lead from a user to a privilege (functionality that enables the user to do something), and are labeled accordingly. In an Oracle path, for example, *U* is user, *R* is responsibility, *M* is menu, and *F* is function.
 - You can expand or contract the size of the image: Click on the square with a horizontal line at the upper left of the frame containing the diagram, and slide it up to enlarge the diagram (and so expose fewer of its objects to view), or down to reduce the diagram (and so expose more of its objects to view).
4. Manipulate information presented by the image:
 - If you move your cursor over any of the objects in a path, the image displays the name of that specific object.
 - If you click on any object in a path, the arrows leading to that object are highlighted in red, distinguishing those paths from others that do not lead to the object you've selected.
 - Because the Results window focuses on a single model, a Highlight Model/Control list box displays only an entry for the model whose results you are reviewing. If, in step 1, you selected paths involving more than one pair of access points, you can select one of those pairs to highlight its paths in red. To do so, first use the Highlight Model/Control list box to select the model. Then click on the downward-pointing icon in the Highlight Conflicting Access Points list box, and select the pair of access points you want. (If, in step 1, you selected paths involving only one pair of access points, only that pair is displayed in the Highlight Conflicting Access Points list box.)
 - You can narrow the focus of the Visualization image by eliminating its first hierarchical level (users whose assignments have generated conflicts), or the first and second hierarchical levels (users and the roles assigned to them). To do so, click on the downward-pointing icon in the list box labeled Chose a simplification level, and select the Hide User option or the Hide User & Role/Permission List option.
5. Select a path that serves as a filter for paths listed in the Results window: Click on any node in the graph. The path to that node appears in the Apply Path Filter field. Click on the Apply button. The Visualization graph closes, and the Results window displays only paths defined by the filter you've selected.

To close the Visualization window without first selecting a filtering path, click on the × symbol in its upper right corner.

Creating and Managing Continuous Controls

Typically, a continuous control defines risk and generates incidents — for AACG, records of access-point assignments that exceed the defined risk. A control may instead define a set of data that is incorporated into a user defined object, which may then be used in transaction models and controls as if it were a business object.

In either case, to create a control a user selects a model; the control adopts its risk definition (filtering logic). The user adds information needed for the control to be applied: whether it is to generate incidents or a dataset; a datasource to which the control is applied; perspective values, and users (associated with those values) who can resolve incidents; a priority; and more. The user also selects an enforcement type — Prevent, Monitor, or Approval Required — that determines what actions may be taken when the control identifies incidents.

A Manage Controls home page presents a list of continuous controls, providing summary information about each. To open the page, select Continuous Control Management in the Navigator, then Manage Controls among the Continuous Control Management tasks. You can see the controls to which your data roles give you access.

Some values are exposed by default, and others are hidden. To display hidden values (or to hide any of those already on display):

1. Right click in the header row of the grid that lists controls.
2. A list of available columns opens. To select a column for display, click on its check box so that a check mark appears. To remove a column from display, click on its check box so that its check mark disappears.
3. Left click anywhere outside of the list of columns to close it.

You can create new controls from models, or edit existing controls. You can evaluate controls, import or export them, and run a report about them. For each control you select, GRC opens a distinct, tabbed page. To return to the Manage Controls page, close the control by clicking its Done button, or click on the Manage Controls tab.

Creating Access Controls

Because every control is based on a model, ensure that at least one access model exists before you attempt to create an access control. You may convert any number of access models into controls at once. If you create more than one, their processing

logic, names, and descriptions remain distinct, but other values are the same for all the controls you create at once.

1. In the Manage Controls home page, click on Actions > Create Access Control.
2. A Create Control: Choose Model window opens.

In an Available Models grid, select models you want to convert into controls: 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 models. A Model logic panel displays the filters that define each model you select; the last model you select is the one whose filters remain on view.

3. Click on the Next button. A Deploy Control: Define Control Details window replaces the Choose Model window. In it, set the following values, as described below: name and description; priority, status, result type, and enforcement type; datasource; perspective values and, with them, users who can investigate control incidents; and comments.

You may click on a Back button, to return to the Choose Model window and revise your model selection. If so, when you return to the Define Control Details window, any values you have selected remain in force.

4. When you are satisfied with all the selections you have made, click on the Submit button in the Define Control Details window.

Naming and Describing Controls

In the Define Control Details window, a Details grid displays a row for each model you selected. Each row contains the name and description of its model. You can accept these as the names and descriptions of the controls you are creating, or click in each Name and Description field to create new values.

Setting Priority, Status, Result Type, and Enforcement Type

In the Priority field, enter a value that expresses the importance of the controls you are creating in relation to others. The value must be a number. (Your company should establish a set of priority values and enforce consistent usage.)

In the Status list box, select Active (the default) to use the controls you create, or Inactive to hold them in reserve.

In the Result Type list box, select “Incidents” if you intend for the controls to generate incidents, or “Dataset” if you intend for the controls to supply data to user defined objects. (A user defined object is a set of data returned by a CCM continuous control that is used as if it were a business object. Although only a transaction model or control can cite a user defined object, either an access or a transaction control can serve as the basis of a user defined object. For more information on creating a user defined object, see the *Oracle Enterprise Transaction Controls User Guide*.)

In the Enforcement Type list box, select Prevent, Monitor, or Approval Required. If users are assigned roles after these access controls are activated, the assignments are denied if they violate Prevent controls, permitted if they violate Monitor controls, or suspended pending approval if they violate Approval Required controls.

Selecting Datasources

The models upon which you are basing the controls you create are already associated with datasources. You may retain those datasources, but if you choose to do so, you must actively select them as you create the controls. Or, you may select new datasources for the controls you are creating.

1. In the Define Control Details window, click on the Manage Datasource button. A Map Datasources window opens, displaying one row for each datasource specified in the models upon which you are basing your controls.
2. In the Mapped Datasources list box of each row, select a datasource appropriate for the environment in which the controls are to be applied.

In each row, a Datasources Used field displays the datasource associated with a source model. You may select this or another datasource in the Mapped Datasources field to apply to controls you are creating.

As you create a model that includes entitlements, you associate the Access Entitlement business object with a Grc datasource. However, if you are converting an entitlement model into a control, you do *not* select the Grc datasource here. Instead, select datasources that contain access points included in the entitlements.

3. Click on the OK button. The Map Datasources window closes, and your selections appear in the Datasource field of the Define Control Details window.

Selecting Perspective Values and Result Investigators

Two sets of perspective values apply to controls and the incidents they generate:

- “Control Perspectives” values apply to the control itself. Users have access to the control if their job roles include data roles associated with these perspective values (and if their duty roles grant privileges to work with controls). Each control inherits, as Control Perspectives values, the values assigned to the model upon which the control is based. As you create the control, you can add to these values (see “Selecting Perspectives” on page 1-4), but you cannot remove the values inherited from the model.

For a control to inherit perspective values from a model, the perspective hierarchy cited by the model must also be associated with the control object (in the Manage Module Perspectives page).

- “Result Management Perspective Assignment” values apply to incidents generated by controls; select them as you create the controls. (See “Selecting Perspectives” on page 1-4.) Users are eligible to review these incidents if their job roles contain both a duty role with the privilege for incident review and a data role associated with perspective values matching those selected here.

As you select perspective values in the Result Management Perspective Assignment panel, GRC users eligible to review incidents become available in the Result Investigator field. In that field:

- Select All Eligible Users to permit incident review by any of those users.
- Select Search to appoint a single user for incident review. A Search and Select Investigator dialog opens. In it, enter text strings to match any combination of

username, given name, and surname. (Once again, you can use the percent sign as a wild-card character.) Then select the user you want.

Writing Comments

To add a comment to the controls:

1. Click on the Add Comments button. A Comments dialog opens.
2. In the Comments dialog, type the comment you want to add to the controls.
3. Click on the Save button. The comment appears in the Comments panel of the Define Control Details window, together with the date, time, and your name.

Mass-Editing Controls

You can modify certain settings — priority, status, comments, perspective values, and result investigator — for any number of existing controls at once:

1. Select the controls you want to modify from the list of controls on the Manage Controls home page: To select a continuous set of controls, 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 controls. Or, make no selection to edit all in a complete or filtered list of controls.
2. Select Actions > Edit. An Edit Controls dialog opens.
3. Modify any or all of the following:
 - Enter a new value for priority (a number value), status (Active or Inactive), or comment. (The controls retain their original values for any of these fields you leave unedited.)
 - In each of the perspectives panels, select perspective values to be added to, or removed from, those already chosen for each control you are editing. Select the Add or Remove radio button, then move the values to be added or removed from the Available Perspective Items list to the Selected Perspective Items list. As before, “Control Perspectives” apply to the controls you are editing, and “Result Management Perspectives” apply to incidents they generate.
 - Choose whether to select a result investigator (see page 3-3). By default, the field is blank; if you make no selection, each control retains the result investigator originally assigned to it. Or, a control defaults to All Eligible Users if its original investigator is invalidated by selections you’ve made for Result Management Perspectives. If you make a selection, it applies to all the controls you are editing. Users available for selection are those whose data roles specify perspective values that are common to the controls you are editing.
4. To complete the edits, click on the OK button.

Viewing and Editing Individual Controls

For each control, you can open a page in which you can view its full details. Or, you can open an edit version of that page, in which you can modify some configuration

details, add comments, or revise perspective-value and result-investigator assignments. (Any number of pages, each devoted to a distinct control, may be open at once, but you must open them one at a time, to avoid triggering the mass-edit feature.)

To open a control in view mode, click on its name in the Manage Controls home page.

To open a control in edit mode, do either of the following:

- Open a control in view mode, then click the Edit button in the view page.
- In the Manage Controls home page, click in the row for the control you want to edit, and select Actions > Edit.

In each of these pages:

- A Details panel displays the name, description, status, priority, and enforcement type of the control. You can modify those values in the edit-mode page; enter values in write-enable fields.
- This panel also displays information that cannot be edited, including the control type and result type; the datasources to which the control applies; dates on which it was created, last run, and last updated; and a revision number.
- A Comments panel displays existing comments. When the page is in edit mode, you can add a comment as you would if you were creating a control (see page 3-4).
- A Control Perspectives panel displays perspective values currently assigned to the control. A Result Management Perspective Assignment panel displays perspective values assigned to control incidents, as well as the current result investigator. In the edit-mode page, you can modify perspective values (see page 1-4) and select a new result investigator (see page 3-3).
- A Control Logic panel displays the filters and (for transaction controls) functions or pattern that define the processing logic of the control, arranged in the AND/OR order in which they are analyzed. These elements cannot be edited.

In the edit-mode page, click the Save button to save your modifications. In either the edit- or view-mode page, click the Done button to close the page.

Running Controls

You can cause GRC to analyze any selection of controls, returning incidents or compiling datasets for user defined objects (depending on the Result Type selected for each control). To begin, choose the controls you want to analyze from the list on the Manage Controls home page: To select one, click on its row. To select a continuous set of controls, 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 controls.

Then, do either of the following:

- Evaluate the selected controls once, immediately. Before doing so, consider synchronizing data from the datasources against which the controls will run; this would ensure that access data is up to date. (See “Synchronizing Data” on page 1-6.) To evaluate the controls, select Actions > Run, or click on the Run button. GRC displays status of the run at the base of the Manage Controls home page.

- Create a schedule on which the selected controls run regularly. To do so, select Actions > Schedule, or click on the Schedule button. A Schedule Parameter dialog opens; in it, enter values that set a name for the schedule, the date and time at which it starts, the regularity with which the controls are evaluated, the date and time (if any) on which the schedule expires, and whether data should be synchronized immediately before each control evaluation. Then click on the Schedule button.

To view the status of a control run, open a Manage CCM Jobs page: select Continuous Control Management under Continuous Monitoring in the GRC Navigator, then select Manage CCM Jobs under Control Administration in the Tasks list. For more on this feature, see “Jobs and Scheduling” in the *Enterprise Governance, Risk and Compliance User Guide*.

Contextual Reporting for Controls

From the Manage Controls home page, you can run a Control Detail Extract Report. For each control, it provides the name, description and comments, type (Access or Transaction), priority, status (Active or Inactive), and number of pending results. It identifies users who created and most recently updated the control, and dates on which they did so. It displays its processing logic; for an access control, this includes any conditions defined for it and entitlements (sets of access points) that belong to it.

To run the report:

1. Select controls upon which you want to focus the report: click on any number of controls (use the Shift or Ctrl key to select continuous or discontinuous sets). If you do not select individual controls, the report includes information about all controls. Or, you can filter the list of controls to include only those you want — for example, a list of controls at a particular priority.
2. In the Report list box, select the Control Detail Extract Report.
3. In the list box immediately to the right of the Report list box, click on the format in which you want to produce the report. The value *csv* produces a file designed for export to another application, such as a spreadsheet, for further manipulation. The value *pdf* produces a formatted report that can be viewed in Adobe Acrobat.
4. Click on the Print button. An Information pop-up window opens, identifying a job number. Note the number, then close the window (click on its OK button).
5. Using the Navigator, go to Tools > Setup and Administration > Manage Jobs. In the Manage Jobs page, locate the row displaying the job ID you noted in step 4. In its Message cell, click on the Job Completed link.
6. A Job Detail window opens. In it, click on the Item Results link.
7. A file-download window offers you options to open or save the report. The precise behavior of this window depends on the web browser you use. In general, if you choose to save, select the Save option. In a distinct save-as dialog, navigate to the folder in which you want to save the file.
8. Close the Job Detail window (click on its OK button).

Resolving Incidents

The evaluation of access controls produces either “detective” or “preventive” results. Preventive analysis (see chapter 5) permits, prevents, or suspends the assignment of roles to users after access controls have been written to define conflicts within those assignments.

Detective analysis uncovers control violations that existed before a given access control is created, and generates “incidents.” Each access incident traces the path through which a user of a business-management application, assigned access points that a control defines as conflicting, can reach one of those access points.

A Manage Results home page presents incidents belonging to the person who is currently logged on to GRC — for your purposes, you. Incidents may belong to you because controls that generate them identify you as a result investigator, or because other investigators have assigned them to you.

The actual resolution of incidents occurs outside of GRC. For example, you may determine that a user’s access to a role should be rescinded if it violates an access control; that action would be completed in the business-management application to which it applies. The GRC Manage Results pages enable you to review incident details, and to set the status of incidents to reflect whether anything should be, or has been, done about them. Moreover, a Simulation feature enables you to preview how resolutions to access incidents would affect a business-management application.

Initially, incidents appear in the Manage Results home page at an Assigned status, which means that you (potentially along with others) have been designated to address them. You can update an Assigned incident to any of the following statuses:

- Accepted, which means you have determined that nothing need be done to resolve the incident.
- Remediation, which means you have decided that some action must be taken in the business-management application to resolve the incident.
- Resolved, which means you have confirmed that the remedial action has been carried out in the business-management application.

GRC may set other statuses:

- Authorized is given to incidents that result from preventive analysis: If a control violation causes the assignment of a role to a user to be suspended, a result inves-

tigator then approves the assignment, and the control is subsequently run, incidents related to the assignment receive Authorized status.

- Control Inactive means that an incident is no longer of concern because the control that generated it has been inactivated.
- Closed indicates that because an incident has been resolved in the business-management application, a subsequent evaluation of controls finds that the incident need no longer be addressed.

An incident has not only status, but also one of three states: In Investigation, Approved, or Closed. A user cannot directly set the state of an incident. He can change its status, then either save or submit it, and GRC assigns a state as a result of these actions. A submission can cause a state change; a save cannot.

In general, if the status of an incident is Assigned or Remediation, its state is In Investigation; if its status is Accepted or Resolved, its state is Approved. However, because of the distinction between saving and submitting a status change, this is not always true. For example, an incident may be at the Remediation status and In Investigation state; a user may update status from Remediation to Resolved; if he saves, rather than submits, the change, the incident remains at the In Investigation state. Or, a Resolved (and Approved) incident may be reopened, its status changed to Remediation. If it is submitted, its state changes to In Investigation; if it is saved, its state remains Approved.

If the status of an incident is Authorized, its state is Approved; if its status is Closed or Control Inactive, its state is Closed.

State matters in part because the Manage Results page presents pending incidents by default, other pages show counts of pending results, and pending incident results are defined as those at the In Investigation state. (State matters also because each user's access is determined by his data roles, which specify states at which he may access data.) To cause the Manage Results page to display incidents at other states (presuming your data roles give you access to data at those states), use standard search features.

Viewing Controls or Incidents in Summary

To review, edit, or assign status to incidents, open the Manage Results home page: select Manage Incident Results from the Result Management tasks available from the Navigator.

From the Manage Results home page, you may navigate to other pages, which show detailed records of individual incidents (see page 4-3). To return from those pages to the Manage Results home page, click on the Manage Results tab.

You can set the Manage Results home page to display either a list of controls that have generated incidents, or a list of incidents generated by those controls. In the control list, each control links to a list of the incidents only it has generated. From any list of incidents, you can open pages that provide details of individual incidents.

- For a list of controls, select Control Summary in the View By list box.
- For a general list of incidents, select Incident Results in the View By list box. For a list of incidents generated by a specific control, click on its Pending Result Count in the Control Summary list.

You can hide or restore the columns that appear in the grids displaying controls or incidents; right-click in the header row of the grid to open a checklist of columns. Those available for incidents include the following:

- **Incident Information.** For an access incident, this is the path through which a user, assigned access points that a control defines as conflicting, can reach one of those access points.
- **Group and Grouping Value fields.** For an access incident, the Group field identifies pairs of access points. pair includes the access point identified in the Incident Information field (at the path specified in that field). Each pair also includes an access point assigned to the user (via a specific path) that the control defines as conflicting with the Incident Information access point. There may be any number of pairs. For access incidents, the Grouping Value field is blank.

Mass-Editing Incidents

You can set status for any number of incidents, or write comments for them, all at once. To do so, first choose the incidents with which you want to work:

1. Generate a list of incidents. (See above.)
2. In that list, select any number of incidents. 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 items. Or, make no selection to edit all in a complete or filtered list of incidents.
3. Select Actions > Edit. A Mass Update dialog opens.
4. Do any of the following:
 - Select the status you want to assign to the selected incidents in the Status list of values. (See page 4-1 for a discussion of status definitions.)
 - Write a comment in the Comments field.
 - Attach files to the incidents (see page 1-6). For a mass edit, you can attach only URLs.
5. Click the Save, Save and Close, or Submit button. (Remember that a submission can alter the state of an incident, but a save cannot. See page 4-2.)

Because the Manage Results home page displays pending incidents by default, incidents disappear from the list if you select a status other than Assigned or Remediation, and submit the change. You can, however, search for incidents at other statuses.

Viewing and Editing Individual Incidents

For each incident, you can open a page in which you can view its full details. Or, you can open an edit version of that page, in which you can set the incident's status, attach files, add comments, reassign the incident, and create relationships between it and EGRCM objects. (Any number of pages, each devoted to a distinct incident, may be open at once, but you must open them one at a time, to avoid triggering the mass-edit feature.)

To open an incident in view mode, generate a list of incidents in the Manage Results home page (see page 4-2), then click on the Result ID value for the incident you want to open.

To open an incident in edit mode, do either of the following:

- Open an incident in view mode, then select Actions > Edit Definition in the view page for that incident.
- Generate a list of incidents in the Manage Results home page, click in the row for the incident you want to edit, and select Actions > Edit.

Each view or edit page includes a Details panel, which displays the name, description, and priority of the control that generated the incident; the current incident status and state; dates on which the control was last run and on which the incident was created and last updated; datasources on which the incident exists; and other details.

Below the Details panel, a set of tabbed panels provides additional information:

- Result Details defines the incident in question: A grid displays the path to an access point that conflicts with another access point, and related information. One column in the grid contains a full expression of the path; others display individual access points within the path, and their type. The related information includes the user who has been assigned the access point that is the focus of this incident, and a grouping value (an access point that conflicts with the one that is the focus of this incident).
- Perspectives shows the perspective values and result investigators currently assigned to the incident. (Initially, these are determined by Result Management Perspective Assignment values selected for the control that generated the incident. You can modify these values (see “Assigning Incidents,” page 4-4).
- Comments displays the comments currently written for the incident, and enables you to create new comments.
- Relationship Assignment lists associations currently configured between the incident and processes, other base objects, risks, or controls in the Financial Governance module or custom EGRCM modules. You can modify these values (see “Assigning Relationships,” page 4-6).

To set status for the incident, open it in edit mode and select a new value in the Status LOV of the Details panel. (See page 4-1 for a discussion of status definitions.) In the details panel, you can also attach files to the incident (see page 1-6). To create a new comment, open the incident in edit mode, click the comments, tab, and click the Add Comments button. An Add Comments pop-up window opens; type your comment and click the OK button. Then save the incident.

When you finish editing an incident, click the Save button or the Submit button. (Remember that a submission can alter the state of an incident, but a save cannot. See page 4-2.) To close the view page for an incident, click its Done button.

Assigning Incidents

If you are the result investigator for an incident, you can assign the incident to another user. You can do this either from the Manage Results home page (in which case you can reassign any number of incidents at once) or from the edit page for an

individual incident. Because eligible investigators are users whose roles specify perspective values that match those assigned to an incident, reassigning the incident may involve resetting the perspective values configured for the incident.

To reassign incidents from the Manage Results home page:

1. Generate a list of incidents in the Manage Results home page (see page 4-2).
2. Select the incidents you want to reassign: To select a single incident, click on its row. 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 the Ctrl key as you click on incidents. Or, make no selection to reassign all in a complete or filtered list of incidents. (You cannot reassign more than 1,000 incidents at a time.)
3. Click on the Assign button. A Perspective Assignment pop-up window opens.
4. Select perspective values to be added to, or removed from, those already chosen for each incident you are reassigning. (See “Selecting Perspectives,” page 1-4.) Select the Add or Remove radio button, then move the values to be added or removed from the Available Perspective Items list to the Selected Perspective Items list. If you are editing incidents with distinct sets of parameter values, you add or remove the same values to or from each set, but you add or remove only those values, and the sets remain distinct.
5. In the Result Investigator field of the Worklist Assignment box, select a result investigator.
 - Select All Eligible Users to permit incident review by any user whose job roles specify data roles that specify perspective values that match those chosen for the incidents. (Incidents default to All Eligible Users if their original investigators are invalidated by your perspective selections.)
 - Select Search to appoint a single user for incident review. A Search and Select Investigator dialog opens. In it, enter text strings to match any combination of username, given name, and surname. (You can use the percent sign as a wild-card character.) Then select the user you want.

By default, the Result Investigator field is blank; if you make no selection, each incident retains the result investigator originally assigned to it. If you make a selection, it applies to all the incidents you are editing.
6. Click on the Submit button.

To reassign an incident from its edit page:

1. Open the edit page for an incident (see page 4-3), and select the Perspectives tab.
2. Select perspective values for the incident. (See “Selecting Perspectives,” page 1-4.) From the incident’s edit page, you directly edit perspective values; those remaining in the Selected Perspectives list are all the values that apply to the incident.
3. Select a result investigator in the Result Investigator field of the Worklist Assignment box. As described above, you can select all users whose roles specify perspective values that match those selected for the incident, or any one of those users.

4. As always when you edit an incident, click the Save button or the Submit button. (Remember that a submission can alter the state of an incident, but a save cannot. See page 4-2.)

Assigning Relationships

You can establish relationships between incidents in the CCM module and objects in EGRM modules. You can relate incidents to processes, other base objects, risks, or controls, which may exist in the Financial Governance module or any custom module. Once a relationship is created, the incident is listed both in the CCM Manage Results page and in a Results tab of the Manage page for the EGRM object to which the incident is related.

From the Manage Results page, you can create relationships for any number of incidents at once. Or, from the edit page for an individual incident, you can create relationships for that incident.

To create relationships from the Manage Results home page:

1. Generate a list of incidents in the Manage Results home page (see page 4-2).
2. Select a set of incidents. To select a single incident, click on its row. 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 the Ctrl key as you click on incidents. Or, make no selection to modify relationships for all in a complete or filtered list of incidents. (You cannot reassign more than 1,000 incidents at a time.)
3. Click on the Assign button. An Assignment pop-up window opens; select its Relationship Assignment tab.
4. Select the Add radio button to add objects to those already chosen for each of the incidents you've selected. Or select the Remove radio button to remove objects from those already chosen. If you are editing incidents with distinct sets of relationships, you add or remove the same objects to or from each set, but you add or remove only those objects, and the sets remain distinct.
5. Select Actions > Add, or click the green + button. A Search and Select window opens.
6. In a Module field, select an EGRM module. In an Object Type field, select a type of object within that module. Click the OK button. The Search and Select window expands to list objects of the type, and within the module, you specified.
7. In that list, select objects with which you want to work. You can search for objects. Again, you can use the Shift or Ctrl key to select continuous or discontinuous sets of objects, or make no selection to accept all in a complete or filtered list.
8. Click the OK button. Objects you've selected then appear in the Related Objects grid of the Relationship Assignment window.
9. If you determine you've added objects to the Related Objects grid erroneously, remove them: Select them and select Actions > Remove, or click the red × button.
10. Click on the Submit button.

To configure relationships from the edit page for an incident:

1. Open the edit page for an incident (see page 4-3), and select the Relationship Assignment tab.
2. Select Actions > Add, or click the green + button. A Search and Select window opens.
3. In a Module field, select an EGRCM module. In an Object Type field, select a type of object within that module. Click the OK button. The Search and Select window expands to list objects of the type, and within the module, you specified.
4. In that list, select objects with which you want to work. You can search for objects. You can use the Shift or Ctrl key to select continuous or discontinuous sets of objects, or make no selection to accept all in a complete or filtered list.
5. Click the OK button. Objects you've selected then appear in the Related Objects grid of the Relationship Assignment window.
6. As always when you edit an incident, click the Save button or the Submit button. (Remember that a submission can alter the state of an incident, but a save cannot. See page 4-2.)

Visualizing Access Incidents

You can generate a graphic depiction of incidents generated by access controls — paths from any number of users to any number of access points involved in conflicts. Select Incident in the View By field of the Manage Incidents page; select any number of access incidents, using the Shift or Ctrl key to select a continuous or discontinuous set; then either click the Visualize button or select Actions > Visualize. A Graph window opens; use it as you would to visualize the results of access models (see “Visualizing Access Results” on page 2-18).

Contextual Reporting for Incident Results

When you select Control Summary in the View By list box of the Manage Results home page, you can generate the following reports:

- Intra-Role Violations by Control Report lists access controls that generate intra-role conflicts for which incidents exist at the Assigned, Remediation, Authorized, or Accepted status. For each control, it also lists the roles for which the conflicts are generated. An “intra-role” conflict is one involving privileges granted by a single role.
- Users with Access Violations by Control Report lists access controls that generated incidents at the Assigned, Remediation, Authorized, or Accepted status. For each control, it lists users whose work assignments have violated the control.
- Result by Control Summary Extract Report lists access and transaction controls that generated pending incidents, and provides information about each control.

When you select Incident in the View By list box of the Manage Results home page, you can generate the following access reports:

- 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.
- 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.
- 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.
- Result Summary Extract Report lists incidents generated by access and transaction controls, providing summary details for each.
- 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.

To run a report:

1. Generate a list of controls or a list of incidents in the Manage Results home page (see page 4-2).
2. Select controls or incidents upon which you want to focus the report. You can do this by clicking on any number of controls or incidents (use the Shift or Ctrl key to select continuous or discontinuous sets). If you do not select individual items, the report includes information about all controls or incidents in the list.

Or, you can filter the list of controls or incidents to include only those you want. For example, you can generate a list of controls at a particular priority, or a list of incidents at a particular status. (If you do not filter incidents for status, the report contains pending incidents — those at the In Investigation state.)

Some incident reports are specific to access or transaction incidents (or controls), and others are general. GRC automatically filters by type as needed: An access-specific report includes information only about access controls or incidents, a transaction-specific report includes information only about transaction controls or incidents, and a general report includes information about both.

3. In the Report list box, click on the report you want to run.
4. In the list box immediately to the right of the Report list box, click on the format in which you want to produce the report. If the report has the word *Extract* in its name, you can select only the value *csv*; this produces a file designed for export to another application, such as a spreadsheet, for further manipulation. For all other reports, you may choose *csv* or *pdf*; the latter produces a formatted report that can be viewed in Adobe Acrobat.
5. Click on the Print button. An Information pop-up window opens, identifying a job number. Note the number, then close the window (click on its OK button).
6. Using the Navigator, go to Tools > Setup and Administration > Manage Jobs. In the Manage Jobs page, locate the row displaying the job ID you noted in step 5. In its Message cell, click on the Job Completed link.

7. A Job Detail window opens. In it, click on the Item Results link.
8. A file-download window offers you options to open or save the report. The precise behavior of this window depends on the web browser you use. In general, if you choose to save, select the Save option. In a distinct save-as dialog, navigate to the folder in which you want to save the file.
9. Close the Job Detail window (click on its OK button).

Using Access Simulation

Simulation enables you to preview how a business-management application would be affected if its configuration were changed so that higher-level access points no longer granted access to lower-level access points, and incidents involving those lower-level access points were therefore resolved. It is a purely visual feature.

A Simulation model enables you to select an access point involved in incidents and display its hierarchy — a diagram showing how the access point connects to all other access points that relate to it as “parents” and “children.” In the diagram, you select parent-child pairs of access points and then “remove” each child from its parent. As you do, the simulation feature builds a remediation plan, essentially listing, as steps, the child access points and the parents from which they would be removed. Once you are satisfied with your plan, you run the simulation and review statistics that show how the removal of the child access points from their parents would impact your incidents, roles, controls, and users. You can print the remediation plan, or save it to your computer.

To create and run a simulation:

1. Name and describe the simulation.
2. Select an access point that’s involved in one or more incidents, and create a graphic model of its hierarchy.
3. Develop remediation steps. In the graphic model, select an access point whose removal might resolve an incident and select its immediate parent. Then select a “Remove” option. Repeat this process as often as you like to create additional remediation steps.

For example, in an Oracle context, a user might have access to functions f1 and f2, and a control may define them as conflicting. You might select f1 and the responsibility through which the user has access to it (assuming there’s a direct link between the two).

4. Run the simulation and view its results.
5. Print a copy of the remediation plan you’ve created, or save a copy.

Creating and Naming a Simulation

To create a simulation:

1. Open the Manage Access Simulations page: select Manage Access Simulations under Incident Management in the Tasks panel.

2. In the Simulations panel, click on Actions > Create New. A new row appears in the Simulations grid.
3. Click in the Simulations field, and type a name for the simulation you are creating.
4. Click in the Description field (or, from the Simulations field, press the Tab key). Then type a brief description of your goal in creating the simulation.

The remaining three fields in the row will be completed by GRC when the simulation is saved; you cannot edit them directly. Creation Date shows the date on which the simulation was created; Owner shows the username of the person who created the simulation; and Last Run shows the date on which the simulation was most recently evaluated (the field is blank if the simulation has never been evaluated).

Creating a Simulation Model

A simulation model applies to incidents generated by one or more user-selected controls. Even so, you would typically want to run synchronization and access analysis on the selected controls before creating a simulation model, to ensure that incidents generated by the controls are up to date.

1. In the Models panel, select controls in the Access Controls field.
Click on the icon that looks like a magnifying glass, to the right of the Access Controls field. A Select Access Controls window opens. Optionally, filter on Name or Status, and click the View button, to search for the control you want to select. From the list that's generated, select one or more controls, using the Shift or Ctrl key to select a continuous or discontinuous set. Then click on the OK button.
2. The grid below the Access Controls field lists access points named in incidents that were generated by the selected controls and that have Accepted, Assigned, or Remediation status. Select an access point around which you wish to build a model.
3. In the Actions menu available from the Models panel, select the Apply option. The space to the right of the Models panel then displays a diagram that shows the selected access point as a central focus, from which radiate all the access points that have any relationship to it. The model diagram shows only those relationships that existed when the data synchronization process was last run.

The simulation model appears as a collection of nodes; arrows show how each node connects to others. As you interpret this diagram, keep the following in mind:

- All nodes represent objects that lead from a user to an access point that enables the user to do something, and are labeled accordingly. In an Oracle path, for example, *U* is user, *R* is responsibility, *M* is menu, and *F* is function.
- If you move your cursor over any of the nodes, the image displays the name of the access point that the node represents.
- If you click on an arrow linking one node to another, the arrow appears in red, to distinguish it from other connections.
- If you double click on any node, the model redraws itself with the selected node as the central focus.

- You can expand or contract the size of the image: Click on the square with a horizontal line at the upper left of the frame containing the diagram, and slide it up its “track” to enlarge the diagram (and so expose fewer access points to view), or down to reduce the diagram (and so expose more access points to view).
- Once you create a simulation model, you can clear it (thus making way to replace it with a model based on some other access point). To do so, select the Clear Model value from the Actions menu available in the Model panel.

Having selected an access point involved in incidents, and created a model around it, you may narrow the model to focus on particular users or roles:

1. Within the model diagram, users and roles are each represented by a single node (labeled *U* or *R*). Click on one of them.
2. In the Actions menu of the Model panel, select Show Users or Show Roles.
3. A pop-up window opens, in which a column lists users with incidents involving the access point upon which the model is based, or roles that provide access to that access point (depending on your selection in step 2). Select (click on) one. If you’ve selected a user, a second column lists roles through which the user has access; if you’ve selected a role, a second column lists users granted access through the chosen role. Make a selection in the second column, so that ultimately you’ve selected a user-role combination.
4. Click on the > button to move your selection to the field all the way to the right.
5. Repeat steps 3 and 4 for each user-role combination you want in your model. If you reconsider, you can select items in the field at the right, then click on the < button to remove them from the field.
6. In the end, each entry in the field at the right displays either a user and a role assigned to her, or a role and a user assigned to it. Click on the OK button, and the simulation-model diagram redraws itself to display only access-point connections appropriate to the selected users and roles.

Developing Remediation Steps

From the graphic model you’ve created, generate steps to remediate incidents:

1. In the simulation model diagram, locate a child access point that you want to exclude from the parent so that the exclusion resolves incidents. Then do any of the following:
 - Single-click on that child and its parent, or on the link between them, and then select Remove from the Actions menu of the Model panel.
 - Double-click on the link between that child and its parent.
 - Hold down the Ctrl key and single-click on the link between the child and parent access points.

A record of the exclusion you created appears in a row in the Remediation Steps panel. In the model diagram, the nodes you selected, and those that descend from them, are grayed out.

2. In the Remediation Steps panel, optionally click in the Comments field of the row you've added, and enter a comment about the step.
3. Repeat steps 1 and 2 any number of times to create additional remediation steps.

Should you change your mind about any remediation step you create, you can use any of several methods to rescind it: In the Model panel, once again select its pair of access points, and then select Revert from the Actions menu; double-click on the link between the access points; or hold down the Ctrl key as you single-click on the link. Or, in the Remediation Steps panel, double-click on the step.

Having generated remediation steps from one graphic model, you can select another access point in the Model panel, develop another model, and create additional remediation steps from it. The steps you create from the original model remain in the simulation. (Any filters you applied to the original model, however, are not saved.)

When you finish creating remediation steps, save the model. Select Save from the Actions menu in the Simulations panel.

Running the Simulation and Viewing Results

To run a simulation:

1. Select the simulation you want to run: Click on its row in the Simulations panel.
2. Select Run Statistics from the Actions menu of the Simulations panel. A progress bar at the bottom of the GRC window tells you when the simulation job is complete.

When the Simulation run ends, select either the Control Violation Count or Incident Path Count radio button in the Statistics panel:

- A control violation is the assignment of duties to one user violating one access control, no matter how many access points may be included in the control and therefore how many ways the user's access may violate the control.
- An incident path is a route by which a user gains access to one of the access points involved in a control violation. If a control defines a conflict between two functions, for example, one path might show how a user's responsibility assignment leads to a menu which leads to one of the functions named by the control.

Almost every control includes at least two access points. (The exception is a specialized "sensitive access" control that may set a single access point in conflict with itself.) Thus there are almost always a minimum of two paths per control violation (one to each of the minimum two access points), and usually very many more. Thus you can expect counts by control violation to be smaller — usually much smaller — than counts by incident path.

Depending on your choice, the Statistics panel displays either numbers of control violations or numbers of incident paths affected by your remediation plan:

- A Total grid displays the number of control violations (or incident paths) that actually exist, the number that would exist if the remediation steps were actually executed, and the difference between the two stated both as an absolute value and a percentage.

- A Users grid lists the users who would be affected by remediation and, for each, states the number of control violations (or incident paths) that actually exist, the number that would exist if the remediation steps were actually executed, and the difference between the two stated both as an absolute value and a percentage.
- A Controls grid lists the controls that would be affected by remediation and, for each, states the number of control violations (or incident paths) that actually exist, the number that would exist if the remediation steps were actually executed, and the difference between the two stated both as an absolute value and a percentage.
- A Remaining Incident Paths grid shows all incident paths remaining — those unaffected by the Simulation. It has User and Control columns for easy filtering and sorting.
- A User and Role Impact grid lists users and roles that would be affected by the simulation. For each, a Type field tells whether the entry is a user or a role, and a User and Roles Impacted field identifies the user or role. The removal of a lower-level access point from a higher-level one may not only resolve an incident. Some users may have legitimate access from the higher-level point to the lower-level one, and implementation of the remediation plan would shut off that legitimate access. This grid lists both types of users (and the roles through which they have access) — those with resolved control violations, and those with lost legitimate access.

Printing or Saving a Remediation Plan

For reference — for example, for use when you actually implement a remediation plan in a business-management application — you can print a remediation plan or save it to your computer. To do so, run the simulation and then select **Actions > View Remediation plan** in the Statistics panel. You are then prompted either to save, or to open and print, a copy of the plan in .PDF format.

Managing Access Approvals

AACG preventive enforcement applies access controls to each user as he is assigned responsibilities in Oracle E-Business Suite, or roles in Oracle Fusion or PeopleSoft. Results depend on what (if any) controls are violated:

- If an assignment generates no conflict, or if it violates a Monitor control, it is allowed. When access is granted even though it has violated a Monitor control, and the control is subsequently run in the GRC Manage Controls page, incidents resulting from that grant appear in the GRC Manage Incidents page, with status set to Assigned.
- If an assignment violates a Prevent control, it is rejected, and no incidents are generated.
- If an assignment violates an Approval Required control, it is suspended until it can be reviewed:

If the control finds conflicts in E-Business Suite or PeopleSoft, GRC notifies result investigators, who use an GRC Manage Access Approvals page to approve or reject responsibilities or roles involved in the conflicts.

If the control finds conflicts in Oracle Fusion, the review is handled by Oracle Identity Management; it's recommended that nothing be done with records of these conflicts that appear in the GRC Manage Access Approvals page. (When conflicts are resolved in Oracle Identity Management, their records are removed from the Manage Access Approvals page. For more on the interaction of Oracle Identity Management and AACG, see the *Oracle Fusion Applications Security Guide*.)

In either case, when an approval decision is made and the control is subsequently run in the Manage Controls page, incidents related to approved responsibilities or roles appear in the Manage Incidents page, with status set to Authorized.

When multiple control violations occur, GRC takes the most restrictive possible action. The “pecking order” is Prevent, Approval Required, Monitor, no conflict. For example, when a role assignment violates a Prevent control and an Approval Required control, access is denied and no notification is sent to result investigators.

When GRC sends notifications of Approval Required control violations, it sends them to addresses recorded for result investigators in the Email Address 1 field of the GRC Manage Users page. Depending on how notifications are configured in the GRC Manage Application Configurations page, notification of the enforcement

outcome may be sent to the user who has been prospectively assigned new duties (see the *Enterprise Governance, Risk and Compliance User Guide*). If so, it's sent to the email address associated with the user in the business application.

A Manage Access Approvals History page in GRC displays a history of assignments that violate access controls of any type.

Assigning Responsibilities in Oracle EBS

In Oracle EBS, the access approvals process begins in the Oracle Users form, as a new user is created or an existing user receives new responsibility assignments:

1. With the Users form open, a system administrator selects a user. He may assign responsibilities in the Direct Responsibilities grid, or review those inherited from newly assigned roles in the Indirect Responsibilities tab. In either case, both the start and end dates for these responsibilities are set by default to the current date, and cannot be modified directly. The administrator saves the new assignments.
2. The administrator clicks on Actions in the menu bar, then on Activate Responsibilities in the Actions menu. An Activate Responsibilities form opens. It presents a copy of the responsibilities listed in the Users form, but allows the administrator to change the end dates.
3. In the Activate Responsibilities form, the administrator removes end dates (or alters them to a future date) for a selection of responsibilities, and so provisionally grants access to them. He then clicks the Initiate Conflict Analysis button.
4. A message, reading "Started Conflict Analysis Successfully," appears. The administrator clicks its OK button to clear it.

Within Oracle EBS, a concurrent request called AACG User Provisioning Poll handles approvals and rejections; it runs periodically, but may be run manually (it takes no parameters). An AACG web service initiates conflict analysis in the access engine. At this point, result investigators may review Approval Required conflicts in the Manage Access Approvals page, or any type of conflict in the Manage Access Approvals History page.

5. If responsibility assignments had violated Monitor controls, or if they had violated Approval Required controls and the resulting conflicts were approved in the Manage Access Approvals page, end dates are removed in the Oracle EBS Users form (or modified to match the setting in the Activate Responsibilities form). The administrator can edit these end dates. If Approval Required assignments were rejected, or assignments had violated Prevent controls, the responsibilities remain end-dated.

Assigning Roles in PeopleSoft

In PeopleSoft, the access approvals process begins in the User Profiles page, as a new user is created or an existing user receives new role assignments:

1. With the User Profiles page open, an administrator creates a user or selects an existing one, then selects the Roles tab. She activates a new row, and selects a role in it; she may repeat this to add any number of roles.

2. The administrator clicks the Save button. A message appears, instructing the administrator to submit a request for review in GRC. The instructor clicks the OK button on this message.

The Roles panel of the User Profiles page returns, but newly added roles have been removed if they are involved in conflicts. At this point, result investigators may review Approval Required conflicts in the Manage Access Approvals page, or any type of conflict in the Manage Access Approvals History page.

3. The administrator clicks on the Run AACG Poller link in the Roles panel of the PeopleSoft User Profiles page. A message states that the Poller has run successfully, and the administrator clicks an OK button to clear it.

She then refreshes the page (navigates away from, and back to, the user account). Roles are restored to the display (and accessible to the user) if they had violated Monitor controls, or if they had violated Approval Required controls and the resulting conflicts were approved in the Manage Access Approvals page. Roles remain deleted if Approval Required conflicts were rejected, or if role assignments had violated Prevent controls.

Although the Run AACG Poller link is activated from a specific user's instance of the Roles panel, it updates role assignments for all users whose role assignments have been resolved in GRC. The Schedule AACG Poller link causes the poller to run regularly at an interval specified in a `pea.properties` file (which is configured during installation; see the *Enterprise Governance, Risk and Compliance Installation Guide* for version 8.6.3). When you select this link, a message states "Successfully started the poller"; click its OK button to clear it. Once selected, the link becomes inactive.

Responding to Notifications

When a response is required — that is, when an Approval Required control has been violated in an Oracle EBS or PeopleSoft instance — result investigators can respond in the Manage Access Approvals page. Any investigator may approve or reject the role assignment, but the first one to do so acts for all; others cannot act after the first investigator has.

It is possible (even likely) for a control violation to involve more than one role, and for the assignment of duties to a user to violate more than one control. In such cases, GRC evaluates all controls, automatically approves access to roles that may be granted without conflict, and displays records of only those roles that would conflict with those already granted.

For example, suppose (in an Oracle EBS context) responsibility `r1` contains function `f1`, `r2` contains `f2`, and `r3` contains `f3`. Suppose further that an Approval Required access control sets `f1`, `f2`, and `f3` in conflict with one another, and that a user is assigned `r1`, `r2`, and `r3`. The user would be granted access to `r1` (if its function, `f1`, happens to be the first one cited in the access control), but not to `r2` or `r3`. A record for the user would appear in the Manage Access Approvals page; it would contain two subordinate records, one each for `r2` and `r3`, with the status of each set to Pending. The result investigator would then approve or reject each of `r2` and `r3`, and submit the decisions.

To approve or reject a user's role assignments:

1. Select Manage Access Approvals in the Result Management list of the Tasks panel.
2. The Manage Access Approvals page opens. Its top portion displays rows containing the user names of users whose assignments have violated controls for which you are a result investigator. Locate the user whose assignment you wish to review, and click on the + symbol next to his name.
3. One or more subordinate rows appear. Each shows a role provisionally assigned to the user, its start and end dates, the EBS or PeopleSoft instance on which the role is assigned, and the assignment status (set initially to Pending). In the Status field of each row, select Approve or Reject. Optionally, type a comment about your decision in the Comments field.
4. If you set the status for any role to Approve, click on the Preview prompt (in the Preview column of the parent row that identifies the user). The lower half of the page then displays records of paths to the access points included in the conflict. Each identifies the violated control, the objects that define the conflict path (the assigned role, the access point included in the control, and path leading from one to the other), and the approver. (If you set the conflict status to Reject, the Preview feature does not apply, and an attempt to run it produces a warning.)

After reviewing conflict paths, you may determine that you should reject the conflict. If so, change the status in the upper half of the Request page to Reject.

5. When you have set status for all provisionally assigned roles to Approve or Reject, click on the Submit prompt (in the Submit column of the parent row that identifies the user, in the upper half of the page). The user's record then disappears from the page.

Viewing Access Approvals History

The Administer Access Approvals page displays records of all users whose responsibility assignments violated access controls of any type. When a user's assignments violate Prevent or Monitor controls, the status of those assignments is set, respectively, to Reject or Approve. When a user's assignments violate Approval Required controls, their status is set initially to Pending. Once the conflict is resolved in the Manage Access Approvals page, the user's records disappear from there, and her responsibility-assignment statuses are reset in the History page to the values (Approve or Reject) selected in the Approvals page.

Users with view permission to the Administer Access Approvals page can review approval history. Users with update permission to this page can both review history and reject role assignments at the Pending status; other statuses cannot be updated. The assumption is that such users would reject Pending roles only under extraordinary circumstances; update rights to the Administer Access Approvals page should be granted sparingly. (View and update rights are, of course, determined by roles assigned to GRC users.)

To open the Manage Access Approvals History page, select Navigator > Tools> Setup and Administration > Administration > Administer Access Approvals. Use the Administer page essentially in the same way as you would use the upper half of the Manage page:

- The page displays rows containing the user names of users whose responsibility or role assignments have violated access controls. Locate the user whose request you wish to review, and click on the + symbol next to his name
- One or more subordinate rows appear, each showing a role assigned to the user, the start and end dates configured for it, the Oracle EBS or PeopleSoft instance on which the role was assigned, the status selected for the assignment, and any comments entered by the user who approved or rejected it.
- If you have view rights, all you can do is review these entries. If you have update rights, then for any row set to the Pending status, you can select a Reject link in the Reject column, and then select a Submit link in the Submit column. The responsibility or role assignment is then end-dated in the Oracle EBS Users form or deleted from the Roles tab on the PeopleSoft User Profiles page.

