Oracle® Application Access Controls Governor

Implementation Guide

Release 8.6.6.1000

Part No. E69145-01

February 2016

ORACLE

Oracle Application Access Controls Governor Implementation Guide

Part No. E69145-01

Primary Author: Stephanie Golly

Contents

1 Application Access Controls Governor Setup Overview 1

Diagnostic Steps 1

Setup Checklist 2

Administration Setup 3

Create Access Models and View Results 4

Set Up Conditions 5

Deploy Controls (Remediation Phase) 5

Manage Access Approvals 7

2 Administration Setup 9

Managing Application Configurations 9

Managing Application Data 9

Running Synchronization 10

Optimizing Synchronization 10

Managing Perspective Hierarchies 10

Managing Roles 11

Managing Users 12

3 Importing Perspectives 13

Preparing a Perspective File 13

Adding Values 14

Adding Perspectives 15

Deleting Values 16

Adding New Values to Existing Perspectives 17

Saving the XML File 17
Importing the Perspective File 18
4 Create Access Models and View Results 19
Importing Content as Models 19
Reviewing Model Logic 20
Managing Access Entitlements 20
Creating Access Models from Scratch 21
5 Model Analysis 23
Model Analysis Checklist 23
Application Access Controls Governor Model Analysis Steps 24
View Results Online 24
Visualization 24
Extract to Excel 24
Initial Remediation 25
Before Deploying a Control 25
Set Up Perspectives in Preparation for Assigning Result Investigators 25
Defining Conditions 26
6 Remediation 29
Analysis and Remediation Checklist 29
Application Access Controls Governor Remediation Steps 32
Run Analysis 32
Focus on Areas with the Highest Risk, Priority, and Volume 32
Review Intra-Role Incidents 33
Review Inter-Role Incidents 34
Use Various On-Line Views to Analyze Incidents 35
Use Various Reports and Extracts to Analyze Incidents 35
Assign Incidents to Business Owners 36
Run Simulation 36
Utilize Corporate Change-Tracking Process 38
Make Changes in the Underlying System 38
Re-evaluate 41

7 Manage Access Approvals 43

Manage Access Approvals Maintenance.....43

Turning Manage Access Approvals Off and On in Oracle EBS...43

Turning Manage Access Approvals Off and On in PeopleSoft....44

Defining Your Notification Schedules 44

8 Methods of Optimizing Performance 45

Hardware/Software Recommendations 45

Filtering Incidents 45

Designing Entitlements.....46

1

Application Access Controls Governor Setup Overview

Oracle Application Access Controls Governor (AACG) is a segregation-of-duties control-authoring and -handling solution that works across heterogeneous platforms to detect and prevent undesired user access.

AACG is one of several applications that share an Oracle Enterprise Governance, Risk and Compliance (GRC) platform. AACG and Oracle Enterprise Transaction Controls Governor run as a Continuous Control Monitoring (CCM) module in the GRC platform. (They are also members of a set of applications known collectively as "Oracle Advanced Controls.") Another application — Oracle Enterprise Governance, Risk and Compliance Manager — may implement a Financial Governance module and other, user-defined modules in the GRC platform. As you set up AACG, you will use software tools specific to it as well as software tools common to it and other applications that share the GRC platform.

Each AACG control specifies "access points" to a company's business-management applications that should not be assigned simultaneously to individual users. AACG then finds users whose duty assignments violate access controls.

Best-practice libraries for PeopleSoft and E-Business Suite provide access models that support rapid segregation-of-duties implementation around common end-to-end business processes. These include Order to Cash, Procure to Pay, Financials, and Human Resources.

Diagnostic Steps

Application Access Controls Governor has been designed to be incredibly scalable by means of hardware configurations. This means AACG performance can often be improved via a hardware change rather than an AACG software change.

Touch points of AACG span hardware, software, and network variables. Refer to the *GRC Suite Certification Matrix* for the preferred and supported hardware configurations. Any deviation from these recommendations may result in unforeseen incidents and would cause additional time and require additional resources during implementation.

It is highly recommended during implementation planning that sufficient time be allocated for setting up, testing, and troubleshooting environment-specific incidents that occur commonly with the many combinations of environments available.

The following is a high-level recommendation for diagnostic steps during environment setup and implementation:

1. Work with Oracle consulting or a partner service provider to evaluate your environment and options for GRC installation.
    a. Consider creating Development, Test, and Production instances. It is highly recommended that the environments for these instances be similar to one another, as varying environments could cause unexpected incidents.
    b. Search for any patches that may need to be applied.
2. Refer to the *Certification Matrix* for preferred and supported hardware configurations.
3. Look on Oracle Support for known environment variable incidents.
4. Follow the *Enterprise Governance, Risk and Compliance Installation Guide* to install GRC.
5. Verify that areas of the application are working (see the *Application Access Controls Governor User Guide* and the *Enterprise Governance, Risk and Compliance User Guide* for more information).
    a. Create a datasource and run synchronization.
    b. Create a simple access control to test (for example, an Oracle responsibility versus itself, so that any assignment of this responsibility would cause a violation).
    c. Run analysis.
    d. View analysis results.
    e. Run a few reports.
6. Continue setups as recommended in this *Implementation Guide*.

Setup Checklist

To set up Application Access Controls Governor, complete the steps in the following checklist.

A two-phase process is assumed:

- During “remediation,” you clean up “incidents” that existed before access controls were created.
- During “access approvals,” existing controls prevent, allow, or suspend new access requests.

Some steps are required, and others are optional. Perform the optional steps only if you are ready to use the features or business functions implemented by those steps.

(Each step is described in further detail later in this document. Moreover, steps may refer to other user documentation in which you can find full information about the procedures for completing each step.)

Administration Setup

- ☐ 1 **Required:** Connect your instance of GRC to its database. Typically, connectivity values are set during installation; you would update the values only if your configuration needs to change. See the *GRC Installation Guide* for more information.
- ☐ 2 **Optional:** AACG can connect, and supply information, to Oracle Fusion GRC Intelligence (GRCI). To use this option, create a distinct schema for its use, known as the "Data Analytics" schema. Then, in an Analytics tab on the Manage Application Configurations page, provide information AACG uses to connect to the Data Analytics schema. See the *GRC Installation Guide* for more information.
- ☐ 3 **Required:** Configure connections to datasources for instances of the business-management applications (such as Oracle EBS or PeopleSoft) that are to be subject to control by AACG. See "Configuring Datasources" in the Application Datasources and Libraries chapter of the *GRC User Guide*.
- ☐ 4 **Required:** Run synchronization to consume the access security model for each datasource. See "Synchronizing Data" in the Application Datasources and Libraries chapter of the *GRC User Guide*.
- ☐ 5 **Optional:** Define perspective hierarchies. Each is, in effect, a set of related values that define a context in which GRC objects may exist. Individual perspective values may be assigned to individual models, controls, and incidents (control violations). Perspectives may then be used for reporting and filtering purposes. For example, a user may generate a report about all controls associated with a particular perspective value. Perspectives are also instrumental in GRC security: data roles define the data to which individual users are granted access, and if associated with perspective values, these roles grant access only to models, controls, and incidents associated with those values.

  GRC Perspective Management enables you to create (or edit) perspectives. Or, Data Migration enables you to import them from a template. (Oracle supplies an import template that includes Business Process and Risk perspectives. You may edit these, or create others, for import.)

  System perspectives for CCM Type, Datasource, Business Object, and User Defined Object secure data. These are not accessible in Perspective Management and cannot be modified directly. Their values are assigned automatically as you choose to create either transaction or access models, and select datasources and business objects for them.
- ☐ 6 **Optional:** Define job, duty, and data roles. In brief, a duty role defines a set of privileges, a data role defines a set of data, and a job role combines duty and data roles to define access that can be granted to users. GRC is seeded with a comprehensive set of roles; if you prefer to use these, it's recommended that you copy seeded roles and use the copies. For complete instructions on working with GRC roles, see the *Enterprise Governance, Risk and Compliance Security Implementation Guide*, as well as the "Security Management" chapter of the *GRC User Guide*.

☐ 7 **Required:** Define AACG users and grant them roles. GRC comes with one configured user, for which both the user name and password are *admin*. This user has rights to all GRC features. By logging on as the admin user, one can create other roles and users. See the *GRC Security Implementation Guide*, as well as the "Security Management" chapter of the *GRC User Guide*.

Create Access Models and View Results

☐ 8 **Optional:** Import content. The AACG export and import functionality may be used to import content in the form of models. During implementation, model logic may be reviewed, results may be generated and analyzed, and the models may (if necessary) be modified before permanent controls are created and used to generate incidents.

Best-practice SOD libraries for PeopleSoft and E-Business Suite may be loaded to support rapid implementation of segregation of duties.

See "Importing and Exporting CCM Elements" in the *AACG User Guide*.

☐ 9 **Optional:** Review model logic. If the best-practice SOD libraries were imported, it is important to review the related entitlements and model logic to ensure the definitions meet your company's expectations for identifying SOD conflicts. You may need to modify these as you see fit.

☐ 10 **Optional:** View model results. The purpose of a model is to allow initial analysis of temporary results *before* permanent incidents are generated. It is also common at this stage to do some initial remediation if your company does not require a history of the incident.

☐ 11 **Optional:** Manage access entitlements. Each is a collection of access points. Typically, those points provide access to functions that are related to one another, and the entitlement name is a business term that reflects the common functionality. To define conflicts, access controls can use entitlements in place of, or in addition to, access points. Each access point in an entitlement is considered to conflict with every point in other entitlements in a control, as well as points included independently of entitlements.

See "Managing and Creating Entitlements" in the Creating and Managing Models chapter of the *AACG User Guide*.

☐ 12 **Required:** Manage access models (or edit those loaded in step 8). An access model may define incidents among any number of access points or entitlements. A single model may mix access-point types — for example, it may include both EBS functions and responsibilities. It may include access points from more than one business-management system, for example defining equivalent incidents in Oracle E-Business Suite and PeopleSoft. It may include both access points and entitlements.

See the Creating and Managing Models chapter of the *AACG User Guide*.

Set Up Conditions

☐ 13 **Optional:** Define conditions to create a more focused analysis and eliminate false positives. You can create three types of conditions:

- You can create condition filters as you create or edit a model. These specify users or other objects, like companies in PeopleSoft or operating units in Oracle EBS, that are exempt from the model (or a control developed from the model). Or they specify circumstances under which the control is enforced — for example, when a user's access to conflicting access points would be granted within a single set of books.
- You can create global conditions. These are essentially the same as conditions configured to apply to an individual model or control, except a global condition applies to all models and controls as they are enforced on a given instance of a business-management application.
- You can create global path conditions. Each excludes one access point from another, such as an EBS function from a responsibility. A path including those points would be excluded from conflict generation. If, for example, a global path condition excluded function1 from responsibility1, a control set function1 in conflict with function2, and a user had access to both functions, no conflict would occur if the user's access to function1 came from responsibility1.

Name the filters descriptively enough to explain the exclusion.

See the Creating and Managing Models chapter of the *AACG User Guide*.

Deploy Controls (Remediation Phase)

☐ 14 **Required:** Create access controls. Deploy controls from models to generate permanent incidents, assigned automatically to appropriate investigators and tracked as they are accepted, rejected, or remediated.

☐ 15 **Optional:** Prioritize controls. Assign numbers to controls to identify which are most important. Consider a company's GRC goals, the regulations it has to follow, areas of high risk to its business, areas on which previous audits have dinged the company, and so on. Prioritization can be used to run focused conflict analysis, sorting, views, and reporting.

See "Creating Access Controls" in the Creating and Managing Continuous Controls chapter of the *AACG User Guide*.

☐ 16 **Optional:** Assign perspective values. For each control, one set of perspective values applies to the control itself. The control inherits these values from the model on which it is based, although a user may add to the inherited values while creating the control. A second set of perspective values characterizes and secures incidents the control generates; these values are selected as the control is created.

See "Selecting Perspectives" in the *AACG User Guide*, and the Perspective Management chapter in the *GRC User Guide*.

☐ 17 **Required:** Select result investigators for controls. Perspective values selected in step 16 determine which users are eligible to be result inves-

tigators — those whose data roles are associated with matching perspective values. By default, each control designates all eligible users as result investigators; you can retain that selection, or choose one of those users.

When roles are assigned to a Oracle EBS or PeopleSoft user after a control has been written to define conflicts within those roles, the assignment may be subject to access approvals. Depending on the control's enforcement types (see step 18, below), a record of the assignment may appear in the AACG Manage Access Approvals page.

Otherwise — if controls are run in other applications, or if access points had been assigned to Oracle EBS or PeopleSoft users before controls were written to define them as conflicting — records of incidents (each the path to an access point involved in a conflict) appear in the AACG Manage Incident Results page.

In either case, violations of a control are reviewed by an eligible user set in the control Result Investigator field. If this Result Investigator field is set to All Eligible Users, any eligible user may review an access request or an incident, but the first to do so acts for all.

See "Selecting Perspective Values and Result Investigators" in the Creating and Managing Continuous Controls chapter of the *AACG User Guide*.

☐ **18** **Required:** Assign enforcement types. During the remediation phase, these suggest what investigators may do about control violations. During the access approvals phase, they determine how violations are handled:

- Prevent: During the access approvals phase, roles are denied to users if they lead to access points a control defines as conflicting. During the remediation phase, this enforcement type suggests that investigators would discontinue the user access represented by the incidents generated by the control.
- Monitor: During the access approvals phase, roles are granted to users even if they lead to access points the control defines as conflicting; associated incidents may appear in the Manage Incidents page for further review. During the remediation phase, this enforcement type suggests that investigators would allow access to continue.
- Approval Required: During the access approvals phase, roles assigned to users are suspended until investigators can review the assignments. During the remediation phase, this enforcement type suggests that investigators would judge whether the user should retain each access point represented by the incidents generated by the control.

See "Creating Access Controls" in the Creating and Managing Continuous Controls chapter of the *AACG User Guide*.

☐ **19** **Required:** Run analysis. Find the incidents that your access controls define. AACG can evaluate all controls or a selection of them, and can evaluate controls immediately or on a schedule. (Consider whether to synchronize data first to ensure that business-management-system data is current and incident generation is up to date.)

See "Running Controls" in the Creating and Managing Continuous Controls chapter of the *AACG User Guide*.

☐ **20** **Required:** Manage incidents. Incidents are automatically assigned to the appropriate investigators. Each investigator can act only on incidents he or she has been assigned. Action on an incident generally requires additional analysis: the running of reports, extracts, and simulations.

See the Resolving Incidents chapter of the *AACG User Guide* and the Reporting chapter of the *GRC User Guide*.

Manage Access Approvals

☐ **21** **Optional:** Engage preventive analysis. Generally, incidents uncovered during remediation have been cleaned up through changes made to access security models of the business systems. Once a company is ready for a preventive approach, it may enable access approvals. Preventive Enforcement Agents (PEAs) are available for Oracle EBS and PeopleSoft systems. In addition, access approvals may be enabled for other business systems.

See the Managing Access Approvals chapter of the *AACG User Guide*.

☐ **22** **Optional**: Configure notifications. When a control generates incidents, AACG may notify the result investigators via your company's email system. For this to happen, establish a connection to the SMTP server your company uses for sending email, and schedule notifications to be sent. This may be done earlier in the implementation; keep in mind, however, that during implementation a high volume of incidents is usually generated.

See "Configuring Notifications" in the Application Configuration Management chapter of the *GRC User Guide*.

2

Administration Setup

Before creating access models or controls, or running them to generate results, use features available in the Tools option of the GRC Navigator to set up your AACG instance. Setup tasks may include configuring performance options and selecting languages in which GRC operates; connecting to datasources (instances of business applications subject to GRC models and controls); configuring perspectives, roles, and users; configuring notifications; and synchronizing data.

Managing Application Configurations

From a Manage Application Configurations page, you can set options that optimize performance. Typically, these properties are set during GRC installation (and all of them are documented fully in the *GRC Installation Guide* and the *GRC User Guide*). Many are not changed subsequently, although others may be modified at any time.

You can also select up to twelve languages in which GRC can display information, set security options, configure an instance of Oracle Fusion GRC Intelligence (GRCI) for enhanced reporting, and set up other features.

Consider your environment and your goals. Will you require various languages? Will you need to create additional reports leveraging the data staging area? What kind of password security does your company require? By carefully evaluating your business needs, you can configure your application accordingly for best performance and reporting.

To set these options, navigate to Tools > Setup and Administration > Setup > Manage Application Configurations. Then select among Properties, Analytics, Security, and other tabs.

Managing Application Data

You must set up one or more datasources in a Manage Application Datasources page. Each datasource is, in effect, a business application subject to access models and controls.

As you select datasources, consider your company's current mandates, risk tolerances, and compliance goals. You may need to connect to development instances

and test instances, and to analyze data across multiple homogeneous instances or heterogeneous platforms.

By carefully evaluating your business needs, you can ensure that when you load or create models and controls, they will run against the appropriate datasources.

(To work with datasources, navigate to Tools > Setup and Administration > Setup> Manage Application Datasources. See the Application Datasources and Libraries chapter of the *GRC User Guide*.)

Running Synchronization

To maximize performance and handle cross-platform analysis, AACG employs synchronization — it extracts access security model data from ERP systems and loads that data into its own database. How often synchronization is run or scheduled depends on various factors.

In general, any time a change is made to the access security model of a datasource against which you are running analysis, you should synchronize access data before you run analysis. If, for instance, your organization commonly makes changes to Oracle EBS menu structures, or creates and changes responsibilities on a daily basis, then it would also be wise to run access synchronization on a daily basis.

If, for another example, your company evaluates incidents on a monthly basis, then it may only be necessary to run the synchronization process once a month.

(You would run access synchronization from the Manage Application Datasources page. The process is documented in both the *GRC User Guide* and the *AACG User Guide*.)

Optimizing Synchronization

A database administrator can generate statistics that quantify the data distribution and storage characteristics of tables, columns, indexes, and partitions. The cost-based optimization approach uses these statistics to calculate the selectivity of predicates and to estimate the cost of each execution plan. *Selectivity* is the fraction of rows in a table that the SQL statement's predicate chooses. The optimizer uses the selectivity of a predicate to estimate the cost of a particular access method and to determine the optimal join order and join method.

Gather statistics periodically for objects where the statistics become stale over time because of changing data volumes or changes in column values. New statistics should be gathered after a schema object's data or structure is modified in ways that make the previous statistics inaccurate. For example, after running synchronization in GRC, collect new statistics on the number of rows and on the average row length.

See *Oracle Database Performance Tuning Guides* for more information.

Managing Perspective Hierarchies

A perspective is a set of related values that define a context in which AACG objects may exist. Values are hierarchical — they have parent-child relationships to one an-

other. Individual values may be associated with individual models, continuous controls, or incident results, in effect cataloging them.

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

Perspectives 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.)

Each model is automatically assigned values for CCM Type, Business Object, and Datasource system perspectives. These values represent selections made by the user who creates the model — whether it is an access or transaction model, and the datasources and business objects selected for it. Thus, at minimum, a model is restricted to users whose data roles include matching values for system perspectives. (A system perspective for user defined objects also exists. However, a user defined object is a set of data returned by a continuous control that is used as if it were a business object in transaction models. User defined objects are not available to access models.)

A user who creates a model may assign other perspective values to it, further restricting its availability.

Each control is developed from a model, and inherits the system perspective values assigned to that model. The control does not inherit other perspective values actively selected by the user who created the model.

A user who creates a control selects two sets of perspective values for it. One set applies to the control itself, determining which users can work with the control. The second set applies to incidents generated by the control, and determines which users are eligible to investigate incidents.

You may consider creating perspectives to secure incidents while you create those that secure models and controls. Or you may wait until you are ready to convert models into controls, when you may have a better idea of who should resolve incidents generated by controls.

Even after models and controls are created, or incidents are generated, you can edit them to modify any of the sets of perspectives associated with them.

GRC Perspective Management enables you to create or edit perspectives. Or, Data Migration enables you to import them from a template (see chapter 3). Once created, a perspective hierarchy becomes available for use with objects of a given type only after it is associated with that type in a GRC Manage Module Perspectives page. For information on managing perspectives and associating them with objects, see the *GRC User Guide*.

Managing Roles

In GRC, duty roles grant access to functionality, data roles grant access to data, and job roles combine duty and data roles to define distinct combinations of privileges that may be granted to users.

Before you begin setting up your roles, consider who will use AACG (and GRC), and for what purposes. Seeded data, duty, and job roles are provided as templates. Common practice is to copy seeded roles and modify them as required.

Examples of roles include:

- Auditors — May be able to review generated conflicts and run reports.
- Internal Controls Group — May help define perspectives, review/create controls, and run reports.
- Business Area/Application Owners — May conduct activities such as creating controls, creating entitlements, viewing incident results, updating status of incident results, and simulating the resolution of conflicts.
- System Administrator — May set up datasources, application configuration, and notification configurations.
- Access Approval Investigator — May review access requests in the Manage Access Approvals panel. (It contains an entry for each occasion when access points are assigned to an Oracle EBS or PeopleSoft Financials user after an Approval Required control has been written to define them as conflicting). According to accepted practice, a user who creates controls should not be able to review the incidents they generate. Therefore the Access Approvals Investigator role typically should not also permit users to create access controls.

(To work with roles, select Setup and Administration under Tools in the Navigator, then Manage Rules under Security. See the *GRC Security Implementation Guide*, as well as the "Security Management" chapter of the *GRC User Guide*.)

Managing Users

Before you begin creating users — during the role creation process — you should have considered who will use AACG, and for what purposes. Consider a naming convention for user names and apply one or more roles to each user as appropriate.

(To set up users, select Setup and Administration under Tools in the Navigator, then Manage Users under Security. See the Security Management chapter of the *GRC User Guide*.)

3

Importing Perspectives

As an alternative to configuring perspective hierarchies in GRC Perspective Management, you may use a Data Migration feature to import perspectives and their values. Data Migration is especially useful for mass creation of perspectives. To use this feature, load perspective data into a "template" (an Excel spreadsheet), and then run an import process against the template.

Apart from system perspectives used for security, no perspectives are seeded with the Continuous Control Monitoring (CCM) module. However, Oracle offers a template that defines two perspectives — Business Process and Risk. You may accept these as they are defined or edit them. You may find it useful to begin with this template as an example for creating your own perspectives and values.

Preparing a Perspective File

The template file for a perspective import consists of three worksheets:

- Perspective: This worksheet contains information needed to create perspectives that, once imported, can be found in Perspective Management (under Tools in the GRC Navigator). Information from the Perspective worksheet populates the Definition section of the page.
- PerspectiveItem: This worksheet contains information needed to establish perspective values. Once imported, these values appear in the Hierarchy tab of the Hierarchy Details section of the Perspective Management page.
- PerspectiveHierarchy: This worksheet determines the hierarchical structure of the perspective. For example, for the Business Process perspective, a Business Process value exists at the highest level, also known as the "root." All other values defined for the Business Process perspective appear as children of the root value. It is possible to have multiple levels in a hierarchy.

The seeded template is called Business Process and Risk Perspective Template.xml. Use it (as is, or with perspectives or values added or deleted) to perform an "initial load" — one for which all data in the file is new to the GRC instance. (You can perform any number of initial loads, but only for all-new perspectives. For an initial load, any data existing in the target GRC instance must be removed from the template.)

Or, generate a template from your GRC instance and use it for an "incremental load" — one that adds values to perspectives that already exist on the GRC instance.

Individual records within worksheets may contain two ID values. For example, the Perspective worksheet contains both a PERSP_TREE_ID and a PERSP_TREE_SYSTEM_ID column. For any column whose heading contains the phrase SYSTEM_ID, be aware:

- For an initial load, in which all data is new, SYSTEM_ID cells must be blank.
- For an incremental load, in which you add values to already-existing perspectives, the SYSTEM_ID for a piece of existing data contains an encrypted value; do not change it. The SYSTEM_ID for any new piece of data must be blank.

You will provide values for other (non-system) IDs, as described in the following procedures.

The following examples demonstrate how to make changes to a template. Note, in particular, that although you can delete values or perspectives from a template, you cannot use Data Migration to delete values or perspectives from those that already exist on a GRC instance.

Adding Values

Define a new value in the PerspectiveItem worksheet, and use the PerspectiveHierarchy worksheet to define its place in a perspective already defined in the Perspective worksheet.

For example, assume you want to add the value "Information Technology" to the Business Process perspective in the Business Process and Risk Perspective Template.xml file.

1. In the PerspectiveItem worksheet, create the new value:
   a. Copy a row in which the PERSP_TYPE_CODE value identifies the perspective to which you want to add a value. (In this example, select a Business Process row — one in which PERSP_TYPE_CODE = GRC_PERSP_BUSINESS_PROCESS). Paste the copy as the last row.
   b. Change entries in the NAME and DESCRIPTION cells to those appropriate for the new value . (In this example, the NAME value is "Information Technology.")
   c. Change the PERSP_ITEM_ID to a unique numeric value.
2. In the PerspectiveHierarchy worksheet, define the new value's place in the hierarchy of values (in this example, a child of the root value).
   a. Again, copy a row in which the PERSP_TYPE_CODE value identifies the perspective with which you are working (GRC_PERSP_BUSINESS_ PROCESS in this example). Paste it as the last row.
   b. Change the value in the CHILD_NAME cell to match the value you added (in step 1b) to the NAME cell of the PerspectiveItem worksheet. (In this example, the value is "Information Technology.")
3. Save the file. Follow verification steps described in "Saving the XML File" (page 17).

Adding Perspectives

Use all three worksheets to define a perspective, define the values it will contain, and define their hierarchical relationships.

For example, assume you want to add a new perspective called "Organization." Its root value will also be "Organization"; its next level is to contain the values "EMEA Unit" and "NA Unit"; each of these is to have Accounting and Production departments as children.

To create this perspective hierarchy:

1. Enter information about the perspective itself in the Perspective worksheet:
   - **a** Copy an existing row and paste it as the last row.
   - **b** Change values in the NAME and DESCRIPTION cells to those you desire. (In this example, the NAME value would be "Organization.")
   - **c** Change the PERSP_TYPE_CODE to a unique value. In this example, that value might be GRC_PERSP_ORG.

     Note, however, that before you import the template, you must use the GRC Manage Lookup Tables feature to create this value as a lookup of the GRCM_PERSPECTIVE_TYPE lookup type. See the *GRC User Guide* for information on managing lookup tables.
   - **d** Change the PERSP_TREE_ID to a unique numeric value.
2. In the PerspectiveItem worksheet, enter information about the root (highest level) value in the perspective hierarchy.
   - **a** Copy an existing row and paste it as the last row.
   - **b** Change the values in the NAME and DESCRIPTION cells to appropriate new values. (In this example, the name would be "Organization.")
   - **c** Change the PERSP_TYPE_CODE to match the one used in the Perspective worksheet (GRC_PERSP_ORG in this example; see step 1c).
   - **d** Change the PERSP_ITEM_ID to a unique numeric value.
3. In the PerspectiveItem worksheet, enter information about all other values in the perspective hierarchy:
   - **a** Copy the row you created in step 2 and paste it as the last row.
   - **b** Change the values in the NAME and DESCRIPTION cells to appropriate new values. (In this example, one name value would be "EMEA Unit.")
   - **c** Change the PERSP_ITEM_ID to a unique numeric value.
   - **d** Repeat these steps for each value you want to add to the perspective hierarchy. (In this example, other name values would include "EMEA Accounting," "EMEA Production," "NA Unit," "NA Accounting," and "NA Production," each in its own row.)
4. In the PerspectiveHierarchy worksheet, establish the relationship between your root value and one of its immediate child values.
   - **a** In the PerspectiveHierarchy worksheet, copy an existing row and paste it as the last row.

b. Set PERSP_ITEM_NAME to the name of the root value you created in step 2 ("Organization" in this example).

c. Set CHILD_NAME to the name of a value that you created in step 3, and that is to be an immediate child of the root value (for example, "EMEA Unit").

d. Set TREE_NAME to name of the perspective you created in step 1 ("Organization" in this example).

e. Because the value you selected as PERSP_ITEM_NAME (step 4b) is the root, set ROOT to Y.

5. Repeat step 4 for all other values that are to be immediate children of the root. (In this example, create a parent/child relationship between "Organization" and "NA Unit.")

6. Define relationships for values at other levels:

a. In the PerspectiveHierarchy worksheet, copy an existing row and paste it as the last row.

b. Set PERSP_ITEM_NAME to the name of a perspective value that is to be the parent of another value (for example, "EMEA Unit").

c. Set CHILD_NAME to the name of the value that is to be the child of the value you just selected (for example, "EMEA Accounting").

d. Set TREE_NAME to name of the perspective you created in step 1 ("Organization" in this example).

e. Because the value you selected as PERSP_ITEM_NAME is not the root, set ROOT to N.

f. Repeat these steps for other lower-level relationships (in this example, "EMEA Unit" to "EMEA Production," and "NA Unit" to each of "NA Accounting" and "NA Production").

7. Save the file. Follow verification steps described in "Saving the XML File" (page 17).

Deleting Values

To remove a value from a perspective, delete the row defining the value from the PerspectiveItem worksheet. From the PerspectiveHierarchy worksheet, delete any rows defining its relationships to other values.

For example, assume you want to delete the value "Logistics" from the Business Process perspective in the Business Process and Risk Perspective Template.xml file:

1. In the PerspectiveItem worksheet, find and delete the row with the Logistics value.

2. In the PerspectiveHierarchy worksheet, find and delete the row with the Logistics value.

3. Save the file. Follow verification steps described in "Saving the XML File" (page 17).

Or, use all three worksheets to delete an entire perspective — the perspective itself, its values, and its relationships. For example, assume you want to delete the Risk perspective from the Business Process and Risk Perspective Template.xml file:

1. In the Perspective worksheet, find and delete the row that defines the perspective you want to delete (in this example, the row with the Risk value).
2. In the PerspectiveItem worksheet, delete all rows in which the PERSP_TYPE_CODE value identifies the perspective you deleted in step 1 (in this example, rows in which this value equals GRC_PERSP_CCM_RISK_TYPE).
3. In the PerspectiveHierarchy worksheet, delete all rows in which the PERSP_ITEM_NAME value identifies the perspective you deleted in step 1 (in this example, Risk).
4. Save the file. Follow verification steps described in "Saving the XML File" (below).

Adding New Values to Existing Perspectives

Once perspectives exist on a GRC instance, you can use Data Migration to add new values to them (although you cannot update existing values). First, export perspectives to which you what to add values; this creates an XML file to be edited. Add values to that file. (You will use the "Incremental Load" option to import the file to the same instance from which you exported it, because the Incremental Load option matches on encrypted IDs in the XML file.)

1. Log on to GRC. In its Navigator, select Setup and Administration in the Tools menu, and then select Data Migration among the Module Management tasks.
2. Click the Create Import Template button.
3. In a Create Import Template pop-up, choose the "With Data — Perspectives Only" option, and click the OK button.
4. GRC generates an XML file. Save it to your machine and open it.
5. Follow the procedure described in "Adding Values" (page 14) to add values to existing perspectives.
6. Save the file. Follow verification steps described in "Saving the XML File" (below).

Saving the XML File

When preparing the XML, be sure of the following:

- Render the PERSP_TYPE_CODE in capital letters with no spaces.
- NAME values cannot exceed 150 characters.
- Be sure all required values are populated. (Each column header declares whether a value is required.)
- Be sure all values respect the data required type. (Each column header defines the data type.)
- If perspectives have user defined attributes (UDAPs) these may need to be populated.
- Avoid using any special characters, including carriage returns.
- Be sure there are no duplicates in the NAME and ID columns in all the worksheets.
- Remove any formatting or formulas you may have added to the worksheet.

- Remove all data filters, if any, from each worksheet.
- Be sure the template is saved as XML Spreadsheet (2003 Excel) or XML Spreadsheet 2003 (*.xml).

In addition, consider the following suggestions:

- Take a backup of the database just prior to running the import process and after all the setup and configuration is complete. This provides the ability to restore the instance and back out the imported data if the data load is not to your satisfaction.
- It is good practice to make a copy of the XML file generated as a backup before adding or changing the data within it in.
- After importing any new perspectives, ensure desired objects such as model, control and result have been associated.
- Ensure that a user is defined to have access to view all the imported data.

Importing the Perspective File

To run the import process:

1. Log on to GRC. In its Navigator, select Setup and Administration in the Tools menu, and then select Data Migration among the Module Management tasks.
2. In the Available Modules grid, select the CCM module. Then click the Import Data File button.
3. In an Import File window, click the Browse button, and navigate to the location of the import file. Select the file, so that its name appears in the field to the left of the Browse button.
4. In the Import File window, select an import method:
    - Select Initial Load if all data contained in the import file is new to the module (even if other perspective data already exists in the module).
    - Select Incremental Load if the import file contains any records that add values to perspectives already existing in the module. (The file may also contain data that is new to the module.)
5. Click the Import button. A message presents a job number. Note the number, then close the message (click on its OK button).
6. Navigate to the GRC Manage Jobs page. (Select Manage Jobs among the Setup tasks in the Navigator.)
7. 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.
8. A Job Detail window opens. In it, click on the Job Results link.
9. Review import statistics, including the number of imported records and validation errors. (If validation errors occur, no data is imported. You would need to correct the errors in the import file, then perform the import once again. You can export validation errors to Excel so that correcting the import file is easier.)

4

Create Access Models and View Results

You may decide to load "content" — libraries of access models built by Oracle for use in E-Business Suite or PeopleSoft. If so, you will have entitlements and models to be reviewed with business owners and compared with the company's goals for governance, risk, and compliance. You may need to delete or edit models and entitlements, or add new ones. At this point, you should have a good idea of the GRC goals of the company and know what areas of the business should be focused on.

In addition, you should have determined who should be able to see what by defining perspective hierarchies and data roles, incorporating those data roles into job roles, and assigning those job roles to appropriate users.

Reviewing each loaded model and its access points is necessary to ensure that the goals of the company are being met. There are several ways to approach defining models and deploying controls. A common approach is outlined in the following steps:

1. Identify GRC goals of the company.
2. Load the best-practice SOD library.
3. Hold workshops with subject matter experts (SMEs) to review models.
4. Create and edit models and entitlements as needed.
5. Analyze model results with SMEs.
6. Carry out initial remediation where possible.
7. Create and prioritize controls.
8. Assign perspectives to secure and categorize controls.
9. Assign result investigators.

Below are detailed instructions for each of the control planning and setup steps outlined in the "Create Access Models and View Results" section of the checklist. There are references to other sections of this guide for more detailed instructions.

Importing Content as Models

Content is available in model form. This gives you the opportunity to review (and edit) model definitions, and view results for relevance within your company, before you deploy the models as controls.

It also increases flexibility in the creation of controls. For instance, does your company have more than one division handling controls? Maybe your company basically wants the same control for its US division and for its Europe division, but requires different investigators to review incidents. You could use one model to deploy two controls, first applying the required conditions to filter only a particular operating unit for instance. In this case, you have to maintain only one set of entitlements, as both controls were deployed from the same model.

Models will also come in handy for your internal and external audits. Auditors will have a starting point for doing some of their own analysis, without disturbing your controls or incidents.

Keep in mind, models are secured by perspectives. To access models, users must have data roles associated with perspective values that match the values assigned to the models.

In PeopleSoft, the PeopleSoft Administrator role gives full access to all menus and pages in the PSAUTHITEM table.

The PeopleSoft Administrator role cannot be viewed, edited, modified, or cloned because it is not defined as other roles are defined. The PeopleSoft Administrator role is hard-coded into every application. You will not find this role if you search for it in the roles component. Note that the PeopleSoft Administrator role does not have access to data. Data security is granted through the primary and row-level permission lists assigned directly to a user profile.

To identify users who have access to this role, search for the PeopleSoft Administrator Role model in the seeded content. Import it and run it as you would any other model.

Reviewing Model Logic

Control logic cannot be modified. Therefore, your only opportunity to review (and edit) the logic by which incidents are generated is in models, from which controls are generated.

Models can be viewed and updated only by users with appropriate access, based on data roles. As you import the best-practice SOD library during an implementation, models are assigned values for three system perspectives: Business Objects, Datasources, and CCM Type (for which the value is Access). To access models, a user must have a data role with at minimum those three system perspectives assigned.

Managing Access Entitlements

If you decided to load the best-practice SOD library, you will have a number of entitlements that already group together common access points, labeled by appropriate business terminology.

At this point, you should have a good idea of the GRC goals of the company and know what areas of the business should be focused on.

Reviewing each loaded entitlement and its access points is necessary to ensure that the entitlements fully cover the known ways that users may access functionality. It

may be easier to first identify models to delete, and then focus on the entitlements within the remaining models for completeness.

For PeopleSoft data specifically, many use cases consider an access point (page) to be an issue only if it is part of a specific access path. For instance, Menu1 > Component1 > Page1 may not be problematic, but Menu1 > Component2 > Page1 is considered a problem. For example, suppose a model is concerned with the approval of journals. In the Journal Entry page, one may both enter and approve a journal, but approval requires access via a certain component. So the model filter that specifies approval access must not merely name the Journal Entry page itself, but must instead define the path to the page that includes that component.

For these scenarios, create user defined access points (UDAPs), which combine access points to define paths. They can be used in entitlements or directly in models. User defined access points may also include user preferences.

Creating Access Models from Scratch

You may find that you need additional models to meet your company's GRC goals. You can create new models at any time, or can even copy existing models where it makes sense to save time.

5

Model Analysis

Model Analysis allows an opportunity for reviewing and tweaking the definition of a potential control before actually creating permanent results. In fact, even some initial clean-up can occur if the company does not require the history of the finding or how it was cleaned up. For instance, in some versions of Oracle EBS many conflict paths are generated because of the "AZN menus." Implementers of AACG often have scripts to exclude these AZN menus in the business system. (Speak with a services consulting team for more information.) Identifying these during model analysis and cleaning them up before a control is deployed and permanent incidents are generated may be acceptable, and even desired by the company.

Model Analysis Checklist

The following checklist provides a more detailed list of steps using Application Access Controls Governor during model analysis.

If you have followed the previous steps, you should be at a point where you have loaded the SOD best-practice library of models, and/or have created some of your own. When you are ready to begin the model analysis process, log on to Application Access Controls Governor and work through these steps to begin analysis.

☐ **1** View results online.

Model results for Application Access Controls Governor include users whose access violates the model, the access paths by which they violate the model, the end access point involved in a conflict, and (if applicable) the entitlement involved in the conflict.

☐ **2** Visualization.

A graphical view of access paths causing conflicts is an easy way to grasp the hierarchy of an access path and the various paths a user has that cause conflicts.

☐ **3** Extract to Excel.

Results can be extracted to Excel for further analysis. The access path is broken out into individual columns that represent each access point in the path. These columns can be used to create pivots in Excel to easily view who has access to what, and how.

☐ **4** Initial remediation (incidents are not tracked).

Initial viewing of model results may offer immediate visibility to obvious areas that require remediation. You can determine if your business requires permanent incidents to be generated before cleanup occurs in the business system, or you may choose to do some housecleaning before deploying your model as a control.

You may find it appropriate to add some global and path conditions to exclude obvious false positives noticed while viewing model results, or adjust the model logic as necessary before deployment as a control.

☐ **5** Deploy as control.

Once you are satisfied that the model identifies segregation of duties incidents as you intend, and you are ready to track incidents and their status permanently, deploy the model as a control.

Application Access Controls Governor Model Analysis Steps

Use the *Application Access Controls Governor User Guide* for help in completing the steps described in the Model Analysis Checklist:

View Results Online

Generally, model results total hundreds of pages. Page through a few to see if users jump out at you as obviously obsolete: consultants who should no longer have access, employees who are no longer with the company or, having switched jobs, no longer have anything to do with the model for which you are viewing conflicting results, etc.

As you page through, you may find Application Developer roles applicable only to the development environment. You might use global conditions to exclude these so you can focus on incidents likely to appear in a production instance.

A specific role might catch your eye — maybe a super user role. Enter a filter to limit your model results and focus on just that role. If it has conflicting access points, then you have already identified what is called an "Intra-Role" conflict. To remediate that conflict you have to clean up the security access of that role/responsibility.

Viewing the model results online is a first step to verifying your model definition is what you intended and to get a glimpse of conflicts that violate that model.

Visualization

In addition to the online view and extracts, a visualization feature provides a graphic hierarchy of the access paths causing conflicts. It enables you to analyze more easily the sometimes long and hard-to-read conflict paths.

Extract to Excel

Many business users are comfortable using Excel for analysis. Model results can easily be extracted to Excel for further analysis, filtering, charting, pivot tables, etc.

AACG model results actually break out the access path causing the conflict into individual columns. This allows for very specific analysis within Excel. For instance, one can easily create a pivot of access paths causing conflicts and determine a remediation plan.

For example, a user might want to analyze a particular responsibility. The user can filter model results for this responsibility and export to Excel.

A user can create a pivot table quickly by the individual access point columns and may discover trends, for example that the main incident involves a particular menu. Or, it may be quickly apparent that an AZN menu should be completely removed from its parent menu.

Initial Remediation

If permanent incidents do not need to be tracked in AACG, you can use your standard corporate tracking system to request these menus to be remediated before a control is ever created. However, if you would like to track an incident, including any comments on your remediation action, then you will want to create a control before doing any cleanup.

Before Deploying a Control

Set Up Perspectives in Preparation for Assigning Result Investigators

At this point, you are just about ready to deploy your models as controls. Before you do, think about who will be involved in the investigation process when incidents are generated. You may need to perform some additional perspective configuration, so that you can assign perspective values to the controls you create, and so direct the incidents they generate to users whose roles specify matching perspective values.

Each control is assigned two sets of perspective values. One applies to the control itself, and the other applies to incidents the control generates. The control inherits the first set from the model upon which it is based (although you may add values to this set). You select the second set — the one that applies to incidents — as you create the control. (After the control is created, you can also edit either set of perspective values.)

For instance, if you have controls handled by certain regions in your company, it may make sense to create a new perspective called Region. In that perspective you may have values such as North America, South America, and Europe. It is possible, for instance, that you have different people in charge of reviewing incidents for the violations that happen in the North and South American regions than you do in the Europe region. You may choose to deploy similar controls with different conditions focusing on specific operating units that fall within those regions.

Continuing with that example, you would then be able to apply different result investigators to each control. You may have an Internal Controls group in charge of reviewing controls in Europe and a different group in charge of reviewing controls in North and South America. Different result investigators could be created and assigned to the appropriate controls.

Another approach might be to assign all incident results generated by the control to a "result manager," who reviews incident results and assigns them to appropriate investigators. For instance, an "Americas" result manager might assign some incidents for that region to investigator Jsmith, and other incidents to investigator Ataylor. The result manager would be required to have an Assign Incident Result privilege.

Yet another approach might be to set the result investigator to All Eligible Users. It would be up to the users to determine which incident results they own, and act on them. So even though Jsmith and Ataylor can both see the incidents, Jsmith knows which incidents he is in charge of, and Ataylor knows which incidents she is in charge of.

Defining Conditions

Conditions help eliminate false positives and create focused analysis runs. Conditions are specific to the application datasource and most likely will be tweaked throughout the remediation process to help focus on different areas as the clean-up process occurs.

What does your company want to consider, or exclude, in its analysis for SOD violations? This determines what conditions should be set and at what level (global, control, or path). For instance, certain users (like developers) may cause hundreds of incidents in a development instance that they would not cause in a production instance. You may want to exclude these users from analysis at certain points of the evaluation.

Oracle EBS Conditions

Common global-condition exclusions for Oracle E-Business Suite are available in the EBS Access Conditions business object. Best business practices for Oracle EBS have been identified below as possible conditions to set up for analysis exclusions.

- Function Query Only: **QUERY_ONLY**

  Exempt functions available from menus that provide query-only access; enforce the access control for other menus that provide write access to the same functions.

- Menu Function Grant Flag: **N**

  Do not apply access controls to functions for which the grant flag is not selected on menus. (If not, the function "belongs" to the menu but does not appear on it and cannot be selected.)

- Responsibility End Date: **Less than or equal to Relative Value 0 Days**

  Users do not have access to menus and functions within responsibilities that have been end dated, therefore there is no reason to include these in conflict analysis.

- User End Date: **Less than or equal to Relative Value 0 Days**

  Users who are not active cannot log into the system, therefore there is no reason to include these in conflict analysis.

- User Responsibility Assignment End Date: **Less than or equal to Relative Value 0 Days**

  Responsibility assignments that have been end dated should not be considered in conflict analysis since the user does not actually have access to those responsibilities.

- Menu Function Prompt: **No Prompt**

  Control violations are excluded if there is no prompt for a menu, submenu, or function that leads to an access point included in the control.

Some attributes in the EBS Access Conditions business object support multi-org access control (MOAC) in Oracle EBS R12:

- "MO: Security Profile" specifies MOAC security profiles that may be exempted from AACG analysis.
- "Within Same MO: Security Profile" specifies MOAC security profiles in which access points must exist for an AACG conflict to exist.
- "Operating Unit" and "Within Same Operating Unit" consider operating units in a MOAC security profile (operating units selected as "Include" on the Organization Security tab of the Security Profile or Global Security Profile form in OEBS).

  If a condition filter uses the Operating Unit attribute to exclude an operating unit that is a member of a security profile, then it is excluded, but conflicts may still be generated for other operating units in that security profile.
- "GL: Data Access Set" specifies General Ledger data access sets that may be exempted from AACG analysis.
- "Within Same GL: Data Access set" specifies General Ledger data access sets in which access points must exist for an AACG conflict to exist.
- "Ledger/Set of Books" and "Within Same Ledger/Set of Books" consider ledgers and ledger sets within a data access set.

  If a condition filter uses the Ledger/Set of Books attribute to exclude a ledger or ledger set that is a member of a data access set, then it is excluded, but conflicts may still be generated for other ledgers or ledger sets in the data access set.

In EBS, security profile, data access set, and other options may be assigned (in the System Profile Values form) at the user, responsibility, or site level. For each option, user is the first-priority selection. A responsibility value applies to users for whom no selection is made. The site value applies to responsibilities and users for which no selections are made. AACG analysis respects this hierarchy.

PeopleSoft Conditions

Common global-condition exclusions for Oracle PeopleSoft are available in the PeopleSoft Access Conditions business object. Best business practices for Oracle PeopleSoft have been identified below as possible conditions to set up for analysis exclusions.

- Account Lock: **ACCT LOCKED**

  When a user's account is locked in PeopleSoft, it is the same as if the user were inactive.
- Display Only: **Yes**

  Display Only is set at the page permission level. Page permissions can be different depending on the Permission List>Menu>Component hierarchy they are used in. Do not apply controls to pages that are display only as users cannot actually transact in these pages.

- Hidden: **Yes**

  Do not apply controls to pages that have been set up as hidden as users cannot actually transact in these pages. Hidden pages are work pages that are associated with derived or work records and are often used in work groups. You can store all of your work field controls there. Create these pages when you want calculations to be performed in the background by PeopleCode that the user does not need to see.

Consider adding control-level conditions where user preferences in PeopleSoft affect the access a user has to a page. For instance, a control may define a conflict involving a page in which purchase orders are approved. (It may conflict, for example, with a page in which POs are created.) However, the control need not generate incidents for users who have access to the approvals page, but whose user preferences do not allow for the approval of POs. To exclude such false positives, add the appropriate filter attribute from the Page Access Configurations business object to the control definition.

6

Remediation

Remediation is the act of cleaning up your application to reduce or eliminate segregation of duties conflicts defined by controls. Segregation of duties means simply that each user should not be assigned access points that controls define as conflicting. Segregation of duties is different for every company (although there may be similarities), so you may need to adjust this common approach based on your company's goals for governance, risk, and compliance.

Analysis and Remediation Checklist

Involving the appropriate people during remediation is key. Different people will be involved at different points, and involving the appropriate people at the appropriate times is imperative. Conflict analysis and clean-up is an iterative process, and although there are various ways to approach remediation, we've outlined a common approach utilizing components of Application Access Controls Governor.

The following checklist provides a detailed list of steps using Application Access Controls Governor during analysis and remediation. When you are ready to begin the remediation process, you log on to Oracle Application Access Controls Governor and work through these steps to begin cleanup in your systems.

☐ **1** Run analysis.

Loading all best practice SOD content and running analysis will provide a quick view of your company's overall SOD health and provide a basis for beginning analysis and prioritization.

☐ **2** Focus on areas with the highest risk, priority, and volume.

Depending on your GRC goals, determine an area to begin analyzing — any category of information on which you want to base your remediation efforts. This may be business process, control, or any other category that produces a large number of incidents.

☐ **3** Review intra-role incidents.

Focusing on intra-role incidents first will inherently clean up potentially hundreds of incidents. (In the context of remediation, "role" means the level of access point that is assigned directly to a business-management-application user, such as a responsibility in Oracle E-Business Suite.)

Many times a role has been built with segregation of duties conflicts within itself. By identifying these incidents and cleaning them up first, you will see an across-the-board effect.

☐ **4** Review inter-role incidents.

In an inter-role incident, a user has access to one or more access points across one or more roles. Sometimes removing an access point from one role will clean up several incidents.

☐ **5** Use various on-line views to analyze incidents.

In the Manage Controls panel, view pending incidents by control, and filter records by various columns including priority and any perspectives you may have identified to help categorize your controls.

In the Manage Incidents panel, view pending incidents in the Control Summary view and drill into any control for a filtered list of incidents. Focus on incidents tied to specific priorities, risks, or business process by creating filters and views to help manage and analyze records.

Try using the Visualization feature to view conflict paths in a graphical format and easily identify inter- and intra-role incidents.

☐ **6** Use reports and extracts to analyze incidents.

Through Control and Incident Management screens, or via Report Management, run reports to analyze data. Use the Access Incident Details Extract report to evaluate data in Excel and create necessary filters and pivot tables to analyze the data.

During analysis and remediation, incidents need to be updated based on various factors and questions: Who needs to look at this incident? Should we categorize or prioritize this differently? Is this incident acceptable? What compensating controls are in place, or need to be put in place? Do we need to remediate this incident, and if so how, and whom would it affect? These steps are outlined in the following section and correspond with the remediation section of the flow chart.

☐ **7** Manage perspectives

Create new perspective hierarchies and perspective values to help secure and categorize your controls and incidents in a manner that helps you as you filter, analyze, and clean up incidents. For instance, if it makes sense to analyze incidents by region, you may consider creating a perspective called Region and adding desired values, such as North America, South America, and Europe.

☐ **8** Manage investigators.

Various people may be required to investigate incidents. Generally, different business owners are interested when different controls are violated. Incidents are assigned to the investigators specified in the Result Investigator field for each control — “All Eligible Users” or a specific one of those users. An eligible user is one whose data roles are associated with perspective values that match perspective values selected for the control.

Note, though, that as the cleanup process continues, many incidents identified in the early rounds of analysis will be automatically closed.

For instance, although you may focus on the cleanup of one user, the removal of a function from a menu may affect many users.

☐ **9** Manage priorities.

Incidents are assigned the priority associated to the control that was violated. You may find that some incidents hold a higher priority than others, and by reprioritizing these, you can create views, filters, reports and extracts that focus on remediation in a desired priority.

☐ **10** Manage status.

Status is used to keep track of what you want to do with an incident. The initial status value is "Assigned." During the remediation phase, investigators of an incident may choose to accept the incident or remediate the incident.

Accepting an incident usually means identifying compensating controls or adjusting global, path, or control-level conditions. Appropriate comments should be made to justify why the incident is being accepted.

☐ **11** Run simulation.

Before actually making changes in the underlying system, you may wish to run the AACG Simulation feature to answer the "what would happen if" questions that come up during analysis.

☐ **12** Utilize your corporate change-tracking process.

Remediation involves making changes in the system being analyzed. For instance, in Oracle E-Business Suite, a menu structure or responsibility may need to be changed. These changes generally first need to happen in a development instance, most likely next in a test instance, and finally in a production instance. It is important to have a change-tracking process to ensure the changes are made from system to system.

Simulation has a Remediation Plan report that can be given to the system administrator responsible for making changes to the access security model.

☐ **13** Make changes in the underlying system.

Using the change-tracking process, request and make changes in the underlying system. For instance, in an Oracle E-Business Suite environment, you may remove a function from a menu that causes conflicts. During this process, the access security model may change, or compensating controls may be put in place. In either case, the result should produce fewer incidents on the next run.

☐ **14** Re-evaluate.

A common approach to remediation is to analyze incidents, prioritize them, add focus with conditions, clean them up, and then re-evaluate. Initial remediation may require new analysis runs to be executed several times in one day or — depending on how long it takes to run through the previous steps — a longer period. Perhaps remediation can be done throughout the week, with a new analysis run at the end of each week to provide a fresh look at where incidents stand.

Application Access Controls Governor Remediation Steps

Use the *Application Access Controls Governor User Guide* for help in completing the steps described in the Remediation Checklist:

Run Analysis

If you followed the model analysis section as recommended, you will have loaded the content as models, reviewed and updated the entitlement and model definitions to ensure they are applicable to your company and you may have even done some initial clean up. At this point, you should have deleted models that do not make sense for your company and deployed those models that do make sense as controls.

When deploying the models as controls — based on the subject matter expert workshops and close interaction with the control investigators who know and understand the control and risk — you should have been able to add a priority and any perspectives that will help you categorize and prioritize controls.

You are now ready to run an analysis. Your company's goals will determine your next steps. If you already know, for instance, that the procure to pay controls are your highest priority (and if you have created a Business Process perspective with a Procure to Pay value), you may choose to run analysis only on controls with that perspective value. If you aren't sure where to focus your efforts first, you may want to run analysis for all controls so that you can see where the greatest volume is by priority or business process, for instance. This may help give you the direction you need to select a focus area to begin remediation on.

Focus on Areas with the Highest Risk, Priority, and Volume

Depending on your company's GRC goals, determine focus areas to begin analyzing. (A "focus area" is any category of information on which you want to base your remediation efforts — perhaps business process, or control, or any other category that produces a large number of incidents.)

- If you have implemented Oracle Fusion GRC Intelligence (GRCI), its Intelligence tab provides many graphs with which you can examine volumes and distribution of incidents and so focus your efforts to address them.
- Use the Control Detail Extract Report to create pivots, filter and summarize data in a variety of ways to determine your focus area.
- In addition to the graphs and extracts, a visualization feature provides a visual hierarchy of the access paths causing conflicts to more easily analyze the sometimes long and hard-to-read conflict paths.

If an initial analysis run returned a high volume of incidents, you should not only decide on a focus area, but also create some filtered views that include only those controls you want to focus on. (For example, if you choose to focus on the priority one, procure to pay business area, filter on that priority and business area then create a view.) This will make it easy to quickly select the records you are analyzing and working to remediate.

Review Intra-Role Incidents

Intra-Role Incidents are caused when access points within the same role conflict. Clean these up first, as the role has been incorrectly set up if it contains access points that conflict with each other. When you start by eliminating intra-role incidents, you may also clean up several inter-role incidents.

1. View Intra-Role Violations by Control Report found in the Report Management task. This gives a high-level view of roles that have conflicting access points within themselves. You may want to focus on controls you have rated as the highest priority.
2. View Access Violations within a Single Role (Intra-Role) Report. For a given role that has conflicting access points within itself, this shows the controls that are violated and their details — including the users and access points with incidents.

   First, use the Intra-Role Violations by Control Report to determine your highest priority controls with intra-role conflicts. Then run this report and focus on cleaning up the roles related to those high-risk controls first.

   A role may be expected to incorporate conflicts. For example, a Purchasing Super User role may incorporate all purchasing functions, including some that conflict, such as the ability to create a purchase order and approve it. Such a role would be assigned sparingly, but might nevertheless be necessary for high-level managers to do their jobs. As a result, AACG permits the creation of a "sensitive access" control — one that sets a responsibility or role in conflict with itself because it provides so much authority that any user should require approval before being granted access to it.

   In most cases, however, a role should not contain access points that conflict with one another. The Access Violations within a Single Role (Intra-Role) report identifies such roles so that conflicts may be removed from them.
3. Within the Manage Incident Results panel, analyze using visualization and various searches to determine when conflicting access points for one role have been violated.
4. Determine how to remediate.

   These reports, along with online analysis, will help to give context to what access an individual role has, along with the users that have those roles. It is up to the business to decide how to remediate those incidents. Generally, the conflicting access points within an individual role should be separated out. One of the conflicting access points may already exist in another applicable role, or potentially a new role will need to be created so that the intra-role conflict can be cleaned up.
5. Simulate.

   Before actually making any changes in your business system, you may want to simulate what would happen if you were to make the change. Navigate to Simulation and exclude an access point to see how your action would impact your conflicts, roles, controls and users.

6. Remediate.

   Following your company change-tracking process, request that the change be made in your business system. For instance, if you decided to remove the Oracle Enter Journals function from the GL_SU_JOURNAL menu, you would need to follow your company process to request this change. Most likely the change would be made in a development instance, possibly then a test instance, and finally the production instance.

7. Repeat. Remediation is an iterative process. Continue to focus on high-priority, high-risk, and high-volume areas to clean up your business system.

Review Inter-Role Incidents

Inter-role incidents can be approached in a similar manner. Inter-role incidents occur when access points conflict with each other across roles for a single user.

1. View Users with Access Violations by Control report. This is a high-level listing of users that violate controls.
2. View Access Violations by User report. This lists the top 10 users with incidents across roles, as well as details for every user that has violated a control, the roles and access points that cause the violation.

   First, use the Users with Access Violations by Control Report to determine your highest priority controls with inter-role conflicts. Then run this report for those controls. By doing so, you will get a list of users that have violated those controls, and will be able to quickly see who has access to more than one role causing conflicts.
3. Within the Manage Incident panel, analyze using visualization and various filters to determine when one use has conflicting access points that span across roles.
4. Determine how to remediate.

   These reports, along with online analysis will help to give context to what conflicting access an individual user has. It is up to the business to decide how to remediate those incidents. Generally, role access may need to be removed from a user or restructuring of a menu related to a role may need to be considered where there is conflicting access points.
5. Simulate.

   Before actually making any changes in your business system, you may want to simulate what would happen if you were to make the change. Navigate to Simulation and exclude an access point to see how your action would impact your conflicts, roles, controls and users.
6. Remediate.

   Following your company change-tracking process, request that the change be made in your business system. For instance, if you decided to revoke a role assignment for a user, be sure to let that user know your plans and be sure this change actually makes it to the production system.
7. Repeat. Remediation is an iterative process. Continue to focus on high-priority, high-risk, and high-volume areas to clean up your business system.

Use Various On-Line Views to Analyze Incidents

In the Manage Controls panel, view pending incidents by control, and filter records by various columns including priority, risk, business process and any other perspectives you may have identified to help secure and categorize your controls.

In the Manage Incident Results panel, view pending incidents in the Control Summary view and drill into any control for a filtered list of related incidents. Focus on incidents tied to specific priorities, risks, or business processes by setting and saving searches to help manage and analyze records.

Try using the visualization feature to view conflict paths in a graphical format and easily identify inter- and intra-role incidents.

Assign status to incidents: The Manage Incident Results grid has functionality to set statuses on each incident. For instance, if a control has been set with the Approval Required enforcement type, the incidents it generates can be accepted or set to remediate in the Manage Incident Results grid. This can be done individually or several at a time. By setting the status here, you can return to the Manage Incident Results grid later to review incidents set to remediate status, or you can run reports for incidents in the remediate status and determine how to clean up your business system. When incidents are remediated in the business system (i.e. a function causing a conflict is removed from a menu) the next time synchronization and analysis are run the status for those incidents that have been cleaned up will automatically be set to a closed status.

Typically, a single investigator would be assigned all the incidents by which a user's role assignments violate a control, so that the user's access can be addressed in a coherent way. However, for enhanced flexibility, investigators may be assigned to individual incidents.

During initial remediation, instead of setting statuses for every incident, you will want to use your corporate change-tracking system to remediate changes in the business system and rerun analysis often. During this iterative process, incidents will begin to dwindle without your having to set a status each and every incident (for instance, you may be focusing on cleaning up the Purchasing Clerk responsibility but by removing the Create Supplier function from that responsibility, you will affect many users and many incidents will automatically be closed the next time synchronization and analysis are run).

Use Various Reports and Extracts to Analyze Incidents

Running a seeded report or extract is another way to analyze incidents and help with remediation. In addition to those reports already mentioned, the following are reports used commonly for the analysis of incidents:

- Result by Control Summary Extract Report

  Use this to get a summary of pending incidents for each control. See the last time the control was run, any comments associated and use as a general summary level report to help determine where to focus your remediation on.

- Access Incident Details Extract Report

  The ability to extract data from the Manage Incident Results screen is for using pivots and filters to slice and dice data in a variety of ways. Generally, you start

with graphs and other summary reports to understand where you should focus. Once you've determined the area on which you want to focus for remediation (i.e., controls, roles, risks, business areas, users or a combination of these), go to the Manage Incident Results screen and enter your filter to view the data to extract. Then select Access Incident Details Extract Report from the drop down and click extract.

Once you have the data in Excel or a similar application, slice and dice the data to view conflicts in a way that will help you with the remediation process. For instance, creating a quick pivot table in Excel is a great way to see where your conflicts are and what paths are causing the incidents.

- Access Point Report

  This report can be used to get conflict path information, which will help lead to access model hierarchies that need to be cleaned up in the system. For instance, if you find that the Access Violations within a Single Role report identifies the Vendors and Payment Actions functions as conflicting access points, you can use the Access Point Report to find the access paths those functions are used in.

Assign Incidents to Business Owners

When a control is violated, all eligible users are able to access the incidents it generates. (Again, users are eligible if their data roles are associated with perspective values that match values assigned to the control.)

GRC generates a worklist for each eligible result investigator. A worklist is a record of incidents generated by a control, as well as a link to the GRC page on which incidents may be resolved. A user sees the worklist if he is a result investigator for the control that generated the incidents; the worklist appears on his home page.

It may be appropriate to reassign incidents to a business owner who is more directly interested in the incidents. When that person logs on to the Manage Incident Results screen, she will automatically view all the incidents assigned to her.

Run Simulation

To aid in cleanup, Application Access Controls Governor enables you to simulate graphically how incident generation would change if configuration of the business-management application were altered, and to create remediation plans from the simulations. Each step in a simulation names an access point that might be excluded from another access point — in Oracle EBS, for example, a function that might be excluded from a responsibility.

A simulation model enables you to select an access point 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. 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 statistics to determine 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, in order to refer to it if you choose actually to implement the plan in your business-management system.

See “Using Access Simulation” in the Resolving Incidents chapter of the *AACG User Guide*.

Recommended Use of Simulation

1. Analyze incidents in the Manage Incidents page, Visualization, and/or various reports.
2. Determine a “child” access point to remove from a “parent” access point.
3. Create a simulation to see how this would impact your incidents:
    - Apply the “child” access point to a simulation model.
    - Filter by user and role to limit what is shown in the model to a readable amount of data.
    - Add a remediation step.
    - Run statistics.
    - Iterate through this process until you are satisfied with remediation steps.

Keep in mind that the access point grid will show all access points involved in incidents of the selected controls. The model shows the entire access security hierarchy of the access point applied. In other words, the simulation model shows the data from the security model of the datasource, regardless of incidents.

The goal of using simulation is to get an idea of:

- What users and roles have access to my modeled access point?
- What access paths is my modeled access point involved in?
- What conflict paths would I clean up if I remove access point A from access point B?
    - What user incidents would that impact?
    - What role incidents would that impact?
    - What controls would that impact?
    - What conflict paths would remain that I still need to work on cleaning up?
    - What other users and roles would I affect, regardless of incidents?
- What is the remediation plan I am comfortable with so I can send it to the person in charge of the business system security model to make the changes?

During simulation, as you view the model hierarchy and add remediation steps, you will find yourself asking the above questions for various access points. You can continue to apply different access points to the model, in essence “redrawing” the model with the newly applied access point while leaving the remediation steps you’ve added intact. The model is a “means to an end” — it is used simply to view the security model hierarchy in various ways to help analyze who has access to what, and how.

Access paths are visually represented in the model. When a child is removed from a parent, access paths that are no longer accessible will be grayed out. Keep in mind that there may be many paths to get to an access point. The access paths are only gray if *all* ways of accessing the access point are eliminated with the remediation steps. Be sure to also consider what is seen on the screen may not be a complete

picture of the access security hierarchy. Look for the arrows on the right and left of each level that allow you to scroll through to see additional access points in the hierarchy. Also keep in mind if you have filtered your model, not all access points may be displayed on the screen.

In some cases the links that show as "gray" can be misleading. For instance, if not all of the access points are displayed on the screen (i.e., you must scroll to them), it is possible that access points "off the screen" that would be remediated and therefore cause their children to be remediated, would still show links as accessible (i.e., not gray). To ensure links are appropriately gray, consider filtering results in the model to show specific users and roles. In the end, the model is just a visual representation of the hierarchy. The statistics will show the accurate results based on the remediation steps.

Utilize Corporate Change-Tracking Process

Remediation will involve making changes in the system that is being analyzed. For instance, in Oracle E-Business Suite, a menu structure or responsibility may need to be changed. These changes will generally first need to happen in a development instance, then most likely in a test instance, and finally in a production instance. It is important you have a change-tracking process to ensure the changes are made from system to system.

Make Changes in the Underlying System

Remediation is the act of making actual changes in the underlying system in which incidents exist. Options for remediation vary depending on the business system. Some common changes that may need to be made in the business system include inactivating users, revoking role assignments, and changing menu structures.

Generally a system administrator type person makes the security model change in the business system. We assume this person is familiar with the best way to implement the remediation steps. For instance, in Oracle EBS, if we have a remediation step that removes function1 from menu1, the system administrator type person has a few ways to do this:

- Function exclusion on responsibility form.
- Uncheck grant flag on menu for that function.
- Remove prompt for that function in that menu.
- Remove entire line for that function in that menu.

Remember, conditions set up in AACG are considered for exclusions in results (i.e., in the Oracle EBS example, prompt, grant flag).

A specific Oracle EBS example to keep in mind is the concept of "same level" menu/functions. Oracle EBS uses this to grant access to functionality via a form menu, for instance. In order for a user to get to the function, he or she must go through another function (i.e., form). It is up to the system administrator to decide the best route to remove the conflicting access. For instance, instead of removing each function in a same-level "sub function" type menu, it might make more sense to just remove the same level menu from the parent menu. Analysis and Simulation are just ways to analyze conflicting user access; it is ultimately up to the system administrator and business owner to come to an acceptable solution for remediating the incident.

As you begin to resolve conflicts by making changes to the underlying business system (or by creating AACG conditions), you may not only close existing incidents, but also create new ones.

An incident focuses on one access point reached through a specific path. In AACG, a Manage Incident Results page displays a record of the incident, in which a field called "Conflicting Access Point" names this focal access point, and an "Incident Information" field specifies one path through which a user may reach it. Depending on the complexity of the control that has generated the incident, however, this access point may conflict with any number of others. In the incident record, a "Grouping" field captures all these conflicts. It displays pairs of access points; in each pair, one is the focal point specified in the Conflicting Access Point field, and the other is one of access points that conflicts with it.

If you alter the business-system configuration to remove an access point and so resolve one of the conflicts, the original issue is closed when you rerun conflict analysis in AACG. However, if other conflicts remain unresolved, AACG creates a new issue. Its Conflicting Access Point and Incident Information fields specify the same focal access point; its Grouping field removes the resolved access-point pair, but continues to list the unresolved pairs.

Suppose, for example, a control sets two entitlements — Approve Purchase Orders and Approve Invoices — in conflict with one another. The Approve Purchase Orders entitlement contains (among others) Oracle EBS functions called Purchase Orders and Releases. The Approve Invoices entitlement contains an Oracle EBS function called Invoice Approve. Thus the Invoice Approve function conflicts with Purchase Orders and with Releases.

Suppose further that a user can access the Invoice Approve function via two paths (through two sets of menus). He also has access to both the Purchase Orders and Releases functions. When the control is run, many incidents may be created. Among them, two incidents focus on the Invoice Approve function — name it as the Conflicting Access Point. The Grouping field for each issue specifies two pairs of access points — Purchase Orders versus Invoice Approve, and Releases versus Invoice Approve. For each, the Incident status is Assigned. In these two issues, only the Incident Information field differs, displaying the distinct paths through which the user can reach the Invoice Approve function.

Incident Information	Conflicting Access Point	Grouping	Incident Status
General Ledger, UK Health Services - Divisional Directors A-General Ledger > GL_SUPERUSER > AP_NAVIGATE_GUI12 > AP_INVOICES_GUI12 > AP_INVOICES_ENTRY_GUI12 > AP_APXINWKB_MENU > Invoice Approve	Invoice Approve	(Purchase Orders)(Invoice Approve)|(Releases)(Invoice Approve)	Assigned
General Ledger, UK Health Services - Divisional Directors A-General Ledger > GL_SUPERUSER > AP_NAVIGATE_GUI12 > AZN_PR_PAYABLES > AP_APXINWKB_MENU > Invoice Approve	Invoice Approve	(Purchase Orders)(Invoice Approve)|(Releases)(Invoice Approve)	Assigned

If you remove the Releases function from the Oracle EBS menus through which this user can reach it, and then synchronize data and rerun conflict analysis, the original incidents remain open at the Assigned status. However, the Grouping field no longer displays the Releases-versus-Invoice-Approve conflict. (The same result would occur if you were to create a global condition to exclude Releases from analysis.)

Incident Information	Conflicting Access Point	Grouping	Incident Status
General Ledger, UK Health Services - Divisional Directors A-General Ledger > GL_SUPERUSER > AP_NAVIGATE_GUI12 > AP_INVOICES_GUI12 > AP_INVOICES_ENTRY_GUI12 > AP_APXINWKB_MENU > Invoice Approve	Invoice Approve	(Purchase Orders)(Invoice Approve)	Assigned
General Ledger, UK Health Services - Divisional Directors A-General Ledger > GL_SUPERUSER > AP_NAVIGATE_GUI12 > AZN_PR_PAYABLES > AP_APXINWKB_MENU > Invoice Approve	Invoice Approve	(Purchase Orders)(Invoice Approve)	Assigned

An incident is closed if all its conflicts are resolved, although the Grouping field for its entry in the Manage Incidents page continues to show conflict pairs that existed at the moment the incident was closed (and none that had been resolved earlier). In our example, suppose that when only the Purchase-Orders-versus-Invoice-Approve conflict remained, you were to remove the Purchase Orders function from menus through which this user can reach it, then synchronize data and rerun conflict analysis. The result would be incident listings in which only the status changes, as shown below. (Note, however, that because the Manage Incidents page displays pending issues by default, you would have to create a view — filter for incidents at the Closed status — to see these entries.)

Incident Information	Conflicting Access Point	Grouping	Incident Status
General Ledger, UK Health Services - Divisional Directors A-General Ledger > GL_SUPERUSER > AP_NAVIGATE_GUI12 > AP_INVOICES_GUI12 > AP_INVOICES_ENTRY_GUI12 > AP_APXINWKB_MENU > Invoice Approve	Invoice Approve	(Purchase Orders)(Invoice Approve)	Closed
General Ledger, UK Health Services - Divisional Directors A-General Ledger > GL_SUPERUSER > AP_NAVIGATE_GUI12 > AZN_PR_PAYABLES > AP_APXINWKB_MENU > Invoice Approve	Invoice Approve	(Purchase Orders)(Invoice Approve)	Closed

Note that if you had removed both the Releases and Purchase Orders functions from the user's menus, and only then synchronized data and rerun conflict analysis, both conflict pairs would appear in the Grouping field for each incident, because both would have existed at the moment the incidents were closed.

Once an incident is closed, the ERP system may be modified so that a conflict is reintroduced. If so, the incident would be reopened at the Assigned status. In our

example, suppose both the Releases and Purchase Orders functions were restored to the user's menus. The result would be listings like those in the first table in this series. The incident would need to be re-evaluated, even if it had been accepted in the past.

Re-evaluate

A common approach to remediation is to analyze incidents, prioritize, add focus with conditions, clean up, and re-evaluate. It is an iterative process. Initial remediation may require new analysis runs to be executed several times in one day or — depending on how long it takes to run through the previous steps — a longer period. Perhaps remediation can be done throughout the week, with a new analysis run at the end of each week to provide a fresh look at where incidents stand. Analysis and remediation are slightly different for every company. This document was intended to provide guidelines and example approaches based on best practices.

7

Manage Access Approvals

Once most cleanup has taken place, and the customer feels comfortable with the incidents that are known to remain, the AACG Manage Access Approvals feature is normally turned on. This feature implements "preventive" SOD analysis — it applies access controls to users as duties are being assigned. It rejects role assignments that violate a Prevent control and accepts assignments that violate a Monitor control (or no control). If an assignment violates an Approval Required control, AACG suspends the assignment and displays an entry for it in a Manage Access Approvals panel, for review by the investigators designated by the control. If an investigator approves, the assignment is allowed; if he rejects, it is disallowed.

In Oracle EBS, the Access Approvals feature applies only to access granted in the Oracle FND Users form. In PeopleSoft, it applies only to the Users Profile page in either Financials or HR.

See the Managing Access Approvals chapter of the *AACG User Guide*.

Manage Access Approvals Maintenance

Initially after installation, a site may wish to run AACG with the Access Approvals feature turned off, so incidents that existed prior to the installation of AACG can be cleaned up before new incidents are addressed. (Moreover, Manage Access Approvals is typically run in a production instance, but not in a test instance.) Thus, it is possible to turn Manage Access Approvals off and on. You would do so in each Oracle E-Business Suite or PeopleSoft instance that is to be subject to analysis by AACG.

To implement Access Approvals in EBS and PeopleSoft, you must not only turn it on, but also create at least one GRC role that incorporates the Manage Access Approvals permission, assign that role to users, and ensure those users' data roles are associated with perspective values that match those set for the controls.

Turning Manage Access Approvals Off and On in Oracle EBS

To turn Manage Access Approvals off in an Oracle EBS instance:

1. Log on to Oracle E-Business Suite.
2. Select GRC Controls in your list of responsibilities. (Ensure first that the GRC Controls responsibility is available to you.)

3. Under the heading Preventive Controls Governor, click on the Form Rules link.
4. A GRC Controls — Oracle Rules form appears. It provides access to three Preventive Controls Governor applications; make sure the Form Rules tab is selected.
5. In the Rule Name field, query for a rule named "User Responsibility Assignment Rules." (Press the F11 key; type the rule name in the Rule Name field; then press Ctrl+F11.)
6. With the rule loaded in the Form Rules form, clear its Active check box. (Clear the one that applies to the entire rule, nearest to the top of the form. Ignore Active check boxes in the Rule Elements section of the form.)
7. Save the rule: Click on File in the menu bar, and then on Save in the File menu.

To turn Manage Access Approvals back on, repeat this procedure, but select the Active check box in step 6.

When communications between AACG and an Oracle EBS instance are interrupted, Access Approvals requests are stored. When communications resume, an Access Approvals concurrent program (called User Provisioning Request Recovery) sends the stored requests to AACG. It takes no parameters, and is typically scheduled to run periodically.

Turning Manage Access Approvals Off and On in PeopleSoft

During GRC installation, a "Preventive Enforcement Agent" (PEA) was installed on the PeopleSoft server. During that installation, properties were set through the use of a PEA installation file. One of these properties was "Enable PeopleSoft PEA," which (presuming Manage Access Approvals is running in the PeopleSoft instance) was set to the value *y*.

To turn Manage Access Approvals off, you must, in essence, reinstall the PeopleSoft Preventive Enforcement Agent with the "Enable PeopleSoft PEA" property set to the value *n*. (All other property values would remain the same.) To complete this installation, see the *Installation Guide*. To turn Manage Access Approvals back on, reinstall the Preventive Enforcement Agent once again, with the "Enable PeopleSoft PEA" property reset to the value *y*.

Defining Your Notification Schedules

Notification schedules determine how often users are notified when incidents are generated. A consolidated email message is generated for each result investigator, showing all violated controls for which no prior notification had been sent. Before creating a notification schedule, consider how often incidents will be generated, and how immediate is the need to review or fix those incidents.

See "Configuring Notifications" in the Application Configuration Management chapter of the *GRC User Guide*.

8

Methods of Optimizing Performance

The following is a list of ways in which a customer can optimize the performance and use of the AACG application. They are listed in order of priority.

Hardware/Software Recommendations

A key to ensuring the optimal performance of AACG is to follow the hardware and software recommendations. The application has been architected in a manner that makes it more readily scalable by simply increasing the memory and processing capabilities of the environment it resides in. This was intentional as it puts more of the performance control in the hands of the customer, who can do so at a nominal cost.

The AACG application and the database it utilizes should be on the same physical box, to address the latency incidents that can exist between hardware components. Because the application processes millions of rows, removing or reducing communication requirements will help enhance the performance.

This should be the easiest way for customers to control the performance of AACG, as they determine the environment to which the application is deployed. A cost-benefit analysis of the hardware versus the improved efficiency of the resources that will work with the software over the next four to five years should easily show a positive return. In fact, considering the cost of consultants that are typically engaged in the initial deployment of the software, the savings could be recouped even during the implementation phase.

Conversely, deviating from the hardware/software requirements will usually result in a negative performance experience.

Filtering Incidents

By default, only eligible users of an incident may view and act on an incident. Also by default, only “Pending” incidents (those with a state of “In Investigation”) are shown. By limiting the records that are initially queried the user should experience better performance than if all records were shown.

Closed records and records in other statuses may be viewed by filtering in the status column of the Manage Incident Results search header.

Designing Entitlements

To reduce the amount of data generated, allow for focused analysis and remediation, and achieve the best performance, it is important to follow the suggested methodology for defining entitlements.

When a control compares one entitlement with another, the end result is basically the cross-product of those entitlements. That is, the control consists of "subcontrols," in which each access point in one entitlement is compared to every access point in the other entitlement.

For instance, assume we have defined two entitlements — General Ledger Setup and Process GL Transactions — to include the following access points (although this would not be recommended):

General Ledger Setup

AP Accounting Flexfield Combinations GUI	Cross-Validation Rules
Assign Flexfield Security Rules	Assign Descriptive Flexfield Security Rules
Assign Key Flexfield Security Rules	Summary Accounts
Suspense Accounts	Consolidation Mappings
Consolidation Mapping Sets	Purge Consolidation Audit Data
Elimination Sets	GIS AutoAccounting Rules
Subsidiaries	Intercompany Transaction Types
Define Transformation Rules	Financial Item
Define Elimination Formulas	Account Hierarchy Editor
AutoPost Criteria	Reversal Criteria
Journal Categories	Concurrent Program Controls
Journal Authorization Limits	Encumbrance Types
Submission Schedules	Storage Parameters
Journal Sources	Tax Options
Statistical Units of Measure	

Process GL Transactions

AP Daily Rates GUI	AP Period Rates GUI
GL Accounts	Generate AutoAllocation
Generate AutoAllocation: Schedule MassAllocation Requests	Generate AutoAllocation: Schedule MassBudget Requests
Generate AutoAllocation: Schedule Budget Formula Requests	Generate AutoAllocation: Schedule Recurring Journal Requests
AutoAllocation Workbench: General Ledger	AutoAllocation Workbench: Projects
Calculate Budget Amounts	Define Budget
Enter Budget Amounts	Enter Budget Journals
Freeze Budgets	Define Budget Organization
Upload Budgets	Budget Transfer
Transfer Consolidation Data Set	Transfer Consolidation Data
Consolidation Workbench	Generate Elimination Sets
Generate Eliminations	Translate Balances

Intercompany Clearing Accounts	Enter Intercompany Transactions
Generate Recurring Intercompany Transactions	Recurring Intercompany Transactions
Enter Journals	Enter Encumbrances
Post Journals	Reverse Journals
Correct Journal Import Data	Delete Journal Import Data
Import Journals	Define MassAllocations
Define MassBudgets	Generate MassAllocations
Generate MassBudgets	Mass Maintenance Workbench
Open and Close Periods	Year-End Carry Forward
Define Recurring Journals	Define Budget Formula
Generate Recurring Journals	Generate Elimination Formulas
Daily Rates	Historical Rates
Period Rates	Common Stock

The Process GL Transactions entitlement has 50 access points, and General Ledger Setup has 29. If we were to set up a control that compares these entitlements — say, General Ledger Setup versus Process GL Transactions — we would in essence have a total of 1,450 subcontrols. There are a few reasons this is not the recommended approach:

- False positives may be created. For instance is it really a conflict if someone has access to “Tax Options” and “Daily Rates”?
- There is no way to prioritize or categorize. When entitlements and controls are broken down and more specific, priorities and perspectives can be assigned so the most important areas are focused on first.
- There is no way to focus on specific incidents to analyze and finally remediate since it has all been grouped as one large control.
- Voluminous amounts of data would be returned each time analysis is run for the control. In general, analysis and remediation happen iteratively; there is no reason to continually identify conflict paths when no remediation effort has even taken place.

An example of entitlements and controls that would avoid these consequences would be the following:

Security Rule Definitions

AP Accounting Flexfield Combinations GUI	Assign Descriptive Flexfield Security Rules
Assign Flexfield Security Rules	Cross-Validation Rules
Assign Key Flexfield Security Rules	

Manage Journals

Enter Journals	Import Journals

Open and Close Periods

Open and Close Periods

One might then create two controls — Manage Journals versus Security Rule Definitions and Manage Journals versus Open and Close Periods.

Generally, entitlements will have between five and ten access points that group together very like functionality. (Note: Consider creating an entitlement even if there is only one access point in the entitlement. If anything should change, such as the addition of another access point, only one entitlement needs to be updated instead of potentially several controls. This of course will require a little more "up-front" work so the cost-benefit should be weighed depending on the likelihood of a change.)

When entitlements are broken down into smaller chunks, focused controls and incidents can be prioritized, categorized, analyzed, and remediated appropriately. For instance, one control may be less risky and less likely than another. By creating the focused control and entitlements, we can deal with the more important, risky controls first.

In addition to these benefits, investigators (those who are in charge of reviewing and potentially approving or rejecting incidents) may be different and thus specifically assigned to the appropriate focused controls. Also, consider managing access approvals. Once you move into a more preventive mode and enable access approvals, you will want the controls routed to the people most concerned with the specific access being requested.

Designing the controls to process in the most efficient manner should also be considered. Although the following control, titled Manage Journals versus General Ledger Setups control, would yield the same results, we lose the benefits mentioned thus far.

Manage Journals

AND

(Security Rule Definitions OR Open and Close Periods)

Following these suggestions should provide the most optimal AACG experience.