Oracle® Application Access Controls Governor

Implementation Guide

Release 8.6.3

Part No. E24373-02

August 2011

ORACLE

Oracle Application Access Controls Governor Implementation Guide

Primary Author: Stephanie McLaughlin

Contents

4 Model Analysis

5 Remediation

6 Manage Access Approvals

Preface

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

This *Implementation Guide* is meant to provide helpful guidance on the usage of the product. Think of this document as a combination FAQ and helpful "Tips and Tricks."

It is a supplement to the official product documentation (such as the *User Guide* and *Installation Guide*), and is not intended to replace it. If discrepancies exist between this *Implementation Guide* and the official product documentation, the guidance and functional commentary provided by official documents supersede any that may be written here.

Disclaimer

The information contained in this document is intended to outline our general product direction and is for informational sharing purposes only, and should be considered in your capacity as a customer advisory board member or pursuant to your beta trial agreement only. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle. This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle software license and service agreement, which has been executed and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

Other Information Sources

My Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/support/contact.html or visit http://www.oracle.com/accessibility/support.html if you are hearing impaired.

Use the My Oracle Support Knowledge Browser to find documents for a product area. You can search for release-specific information, such as patches, alerts, white papers, and troubleshooting tips. Other services include health checks, guided lifecycle advice, and direct contact with industry experts through the My Oracle Support Community.

Oracle Enterprise Repository

Oracle Enterprise Repository provides visibility into service-oriented architecture assets to help you manage the lifecycle of your software from planning through implementation, testing, production, and changes. In Oracle Fusion Applications, you can use the Oracle Enterprise Repository for:

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

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

Documentation Accessibility

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

Comments and Suggestions

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

1

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. It runs in an Enterprise Governance, Risk and Compliance Controls platform, which it shares with another application called Enterprise Transaction Controls Governor (ETCG). As you implement AACG, you will use software tools specific to it as well as EGRCC software tools common to the two applications.

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 Fusion, PeopleSoft and E-Business Suite provide access controls 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 *Compatibility Matrix* document 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:

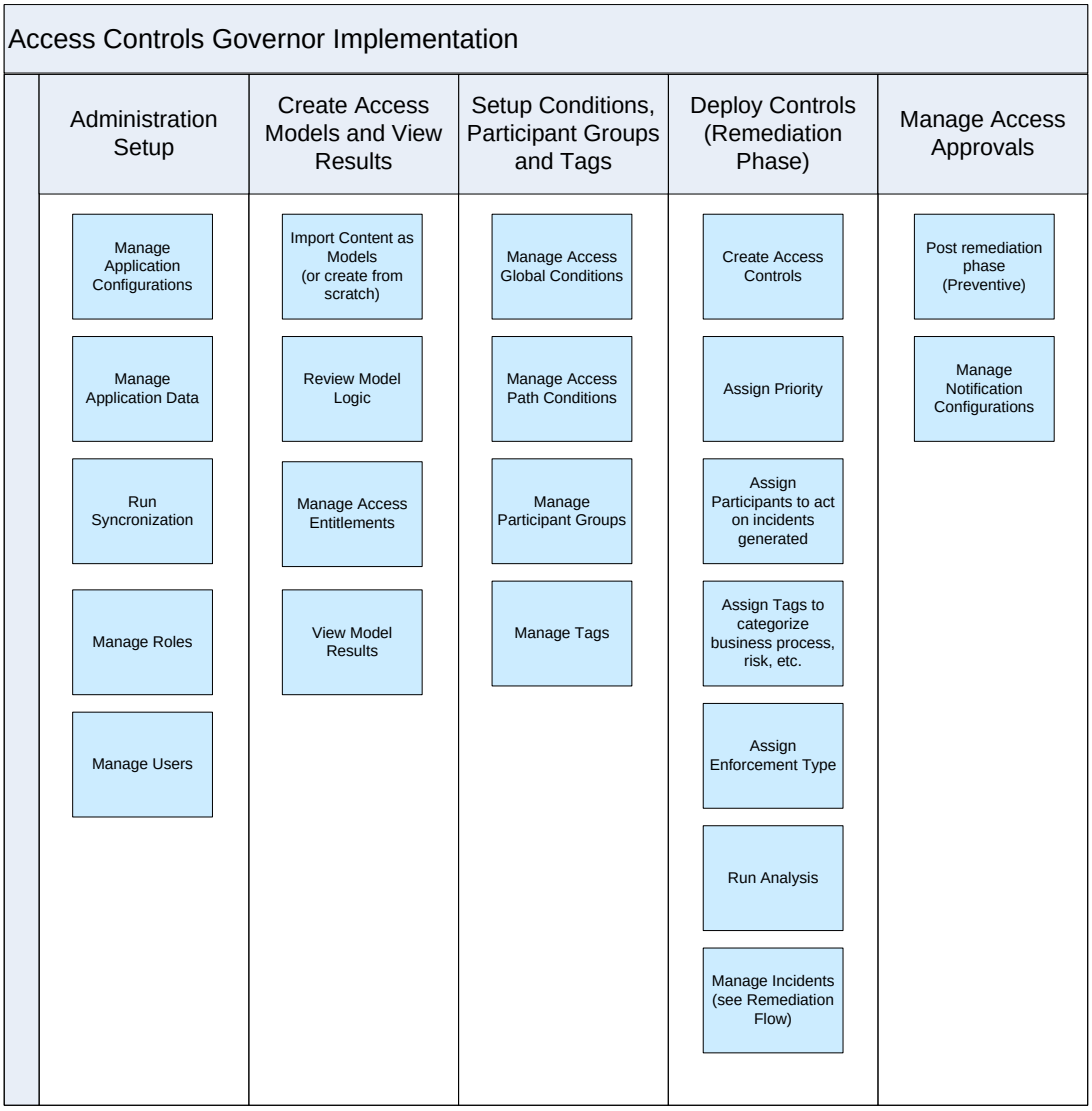
1. Work with Oracle consulting or a partner service provider to evaluate your environment and options for EGRCC installation.
    a. Consider creating Development, Test, and Production instances. It is highly recommended that the environments for these instances be similar to one another, as varying environments could cause unexpected incidents.
    b. Search for any patches that may need to be applied.
2. Refer to the *Compatibility Matrix* for preferred and supported hardware configurations.
3. Look on Oracle Support for known environment variable incidents.
4. Follow the *Governance, Risk and Compliance Installation Guide* to install EGRCC.
5. Verify that areas of the application are working (see the *AACG* and *EGRCC User Guides* for more information).
    a. Create a datasource and run ETL 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*.

Application Access Controls Governor Setup Flowchart

You can set up Application Access Controls Governor in many ways. We recommend the order suggested in the following flowchart. It assumes a two-phase analysis:

- 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; you would perform the optional steps only if you are ready to use the features or business functions implemented by those steps.



Setup Checklist

To set up Application Access Controls Governor, complete the steps in the following checklist. You must complete the steps identified as required; you would complete each of the optional steps only if you want to use the functionality implemented by that step.

(Each step is described in further detail later in this document. Moreover, the description for each step includes a reference to a section and chapter of the *User Guide* for Application Access Controls Governor or for Enterprise Governance, Risk and Compliance Controls, in which you can find full information about the procedures for completing each step.)

Administration Setup

☐ 1 **Required:** Connect your instance of EGRCC to its database. Typically, connectivity values are set during installation; you would update the values only if your configuration needs to change.

See “Setting Properties” in the Data and System Administration chapter of the *EGRCC User Guide*.

☐ 2 **Optional:** Oracle supplies AACG report templates that run in Oracle BI Publisher. You can modify the layouts of these templates to produce reports suited to your circumstances. In addition, AACG can connect, and supply information, to Oracle Governance, Risk and Compliance Intelligence (GRCI). If you choose to use either (or both) of these options, you would create a distinct schema for their use, known as the “Data Analytics” schema. Then, in an Analytics tab on the Manage Application Configurations page, you would provide information EGRCC uses to connect to the Data Analytics schema.

See “Setting Properties” in the Data and System Administration chapter of the *EGRCC User Guide*.

☐ 3 **Required:** Configure connections to datasources for instances of the business-management applications (such as Oracle or PeopleSoft) that are to be subject to control by AACG.

See “Configuring a Datasource Connection” in the Data and System Administration chapter of the *EGRCC User Guide*.

☐ 4 **Required:** Run “synchronization” to consume the access security model for each datasource.

See “Synchronizing Data” in the Data and System Administration chapter of the *EGRCC User Guide*.

☐ 5 **Optional:** Define roles and permissions available to AACG users. To create a role, you essentially give it a name and then select a set of properties for it. The properties grant update or view rights to EGRCC pages you can open from the Tasks panel.

In addition, permissions need to be granted for the datasources and business objects available during model and control creation.

EGRCC comes with two roles already defined — Basic provides access only to a Home panel, and Admin provides access to all (AACG and ETCG) features.

Thus role creation is optional because you may use the existing Admin role to grant access to all the features you will need initially.

See “Creating a User Role” and “Creating a Group Role” in the User and Role Administration chapter of the *EGRCC User Guide*.

☐ 6 **Required:** Define AACG users and grant them roles. EGRCC comes with one configured user, for which both the user name and password are *admin*. This user is assigned the Admin role and so has rights to all EGRCC features. By logging on as the admin user, one can create other roles and users. However, it is imperative for proper security that an

authoritative user modify the admin user's password as soon after installation as that task can be completed.

See "Creating User Accounts" in the User and Role Administration chapter of the *EGRCC User Guide*.

Create Access Models and View Results

☐ 7 **Optional:** Import content. The AACG export and import functionality may be used to import content in the form of models, controls, or templates. During initial implementation, it is recommend that you import models or templates, so that 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 Fusion, PeopleSoft and E-Business Suite may be loaded to support rapid implementation of segregation of duties.

See "Exporting and Importing Models and Templates" in the Creating and Managing Models chapter of the *AACG User Guide*.

☐ 8 **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.

☐ 9 **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.

☐ 10 **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*.

☐ 11 **Required:** Manage access models (or edit those loaded in step 7). An access model may define incidents among any number of access points or entitlements. A single model may mix differing access-point types — for example, it may include both Oracle 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 Enterprise. It may include both access points and entitlements.

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

Set Up Tags, Participant Groups, and Conditions

☐ **12** **Optional:** Define tags. A tag is a category of values. Its values may be assigned to access controls (and so to incidents generated by those controls). Or, its values may be assigned to entitlements (see step 10), and so to incidents generated by controls that include those entitlements. They flag items, and so distinguish them from unrelated items.

See sections devoted to managing tags and assigning them to entitlements or controls in the Creating and Managing Models and Creating and Managing Controls chapters of the *AACG User Guide*.

☐ **13** **Optional:** Create participant groups. Easily manage and assign groups of EGRCC users who are in charge of reviewing and acting on incidents that are generated from controls.

See "Creating Participant Groups" in the Creating and Managing Controls chapter of the *AACG User Guide*.

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

- As you create or edit a model, you can create filters for it. These are "conditions" in that they specify users or other objects, like companies in PeopleSoft or operating units in Oracle EBS, that are exempt from the control. Or they specify circumstances under which the control is enforced — for example, only 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 Oracle 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)

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

☐ **16** **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 Controls chapter of the *AACG User Guide*.

☐ 17 **Required:** Select participants for controls. Each control must assign at least one participant or participant group to resolve control violations.

When roles are assigned to a Fusion, 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 type (see step 19, 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 Fusion, 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 Incidents page.

In either case, violations of a control are reviewed by a participant for whom an “Assign Incidents” property is set to yes. The control may have more than one such participant. If so, any may review an access request or an incident, but the first to do so acts for all.

Note: As a Fusion business process, remediation routing and approval/rejection responses are handled by Oracle Identity Management. The AACG Manage Access Approvals screen and the participants assigned to controls and incidents are not used for Fusion-sourced user access requests.

If no participant is selected for a control, AACG appoints the user who is currently logged on as the “Assign Incidents” participant.

See “Selecting Participants” in the Creating and Managing Controls chapter of the *AACG User Guide*.

☐ 18 **Optional:** Assign tags to categorize controls. As you create controls or entitlements, you can assign tag values to them. There are two seeded tags, Business Process and Risk. By assigning tag values to your controls, you will have different ways to view the conflicts that are generated. This will help you to focus on areas of concern during remediation.

See “Managing Tabs” in the Creating and Managing Controls chapter of the *AACG User Guide*.

☐ 19 **Required:** Assign enforcement types. During the remediation phase, these suggest what participants 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 participants 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 participants would allow access to continue.

- Approval Required: During the access approvals phase, roles assigned to users are suspended until control participants can review the assignments. During the remediation phase, this enforcement type suggests that participants would judge whether the user should retain each access point represented by the incidents generated by the control.

  As noted earlier, for Fusion-sourced user access requests, remediation routing and approval/rejection responses are handled by Oracle Identity Management. The AACG Manage Access Approvals screen and the participants assigned to controls and incidents are not used for Fusion-sourced user access requests.

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

☐ **20** **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 Controls chapter of the *AACG User Guide*.

☐ **21** **Required:** Manage incidents. Incidents are automatically assigned to the appropriate participants. Each participant can act only on incidents they have been assigned. Action on an incident generally requires additional analysis: the running of reports, extracts, and simulations.

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

Manage Access Approvals

☐ **22** **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. Fusion Oracle Identity Management is integrated with AACG, and 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*.

☐ **23** **Optional**: Configure notifications. When a control generates incidents, AACG may notify the control participants 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 Data and System Administration chapter of the *EGRCC User Guide*.

2

Administration Setup

You need to create and set up one or more datasources in the Manage Application Data screen. The datasources you set up depend on various factors, such as your company's current mandates, risk tolerances, and compliance goals. Considerations include the need to connect to development instances and test instances, and to analyze data across multiple homogeneous instances and/or heterogeneous platforms. Below are detailed instructions for each of the planning and installation steps outlined in "Administration Setup" section of the checklist. There are references to other sections of this guide for more detailed instructions.

Use the *Enterprise Governance, Risk and Compliance Controls User Guide* for help in completing setups.

Managing Application Configurations

Before you begin setting up your application configurations, 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 the best performance and reporting needs.

See "Configuring EGRCC" in the Data and System Administration chapter of the *EGRCC User Guide*.

Managing Application Data

Questions asked in the Manage Application Configurations section will also help when setting up your datasources. By carefully evaluating your business needs, you can create the necessary datasources so that when models and controls are loaded or created, they will be able to run against the appropriate datasources.

Create the necessary datasources and set the appropriate application configurations so that when models and controls are loaded or created, they will be able to run against the appropriate datasources in the most optimal manner.

Running Synchronization

To maximize performance and handle cross-platform analysis, application access security model data is extracted and loaded into EGRCC to be used in analysis. How often synchronization is run or scheduled depends on various factors.

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

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.

You should 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 ETL in EGRCC, collect new statistics on the number of rows and on the average row length.

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

Managing Roles

Before you begin setting up your roles, consider who will use AACG (and EGRCC), and for what purposes. Examples of roles may include:

- Auditors — May be able to review generated conflicts and run reports.
- Internal Controls Group — May help define tags, review/create controls, and run reports.
- Business Area/Application Owners — May conduct activities such as creating controls, creating entitlements, viewing conflicts, updating conflict statuses, and simulating the resolution of conflicts.
- System Administrator — May set up datasources, application configuration, and notification configurations.
- Access Approval Participants — 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 Participant role typically should not also permit users to create access controls.

Managing Users

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

3

Create Access Models and View Results

You may decide to load the best-practice SOD library. By doing so, you will have a number of entitlements and models to be reviewed with appropriate business owners, and compared against the company's goals for Governance, Risk, and Compliance. It may be necessary 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.

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. Define and assign tags to categorize controls.
9. Assign control participants.

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 or Templates

We recommend loading the content as models versus controls as this gives you a chance to review (and update) the model definitions and view the results for relevance within your company before deployment as controls.

You may find other helpful reasons to have models as your starting point for imported content. 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 participants 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 not associated to any tags so the seeded business process values are not imported with the models. You will need to categorize your controls when you deploy them.

Reviewing Model Logic

Control logic cannot be modified. Therefore, reviewing the model logic for relevance is your chance to make any necessary changes.

Models can be viewed and updated only by the user who creates them. We recommend that as you import the best-practice SOD library during an implementation, you create a role and user specifically for these models. For instance, create a role and user called *model_implementor* and grant rights only to the access model page.

Users involved in the implementation can log in using the *model_implementor* ID. So can an auditor who would like to use a model imported during implementation.

Another option is to import the content as templates. Templates can be viewed by anyone. If you go this route, users will need to create models from templates.

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.

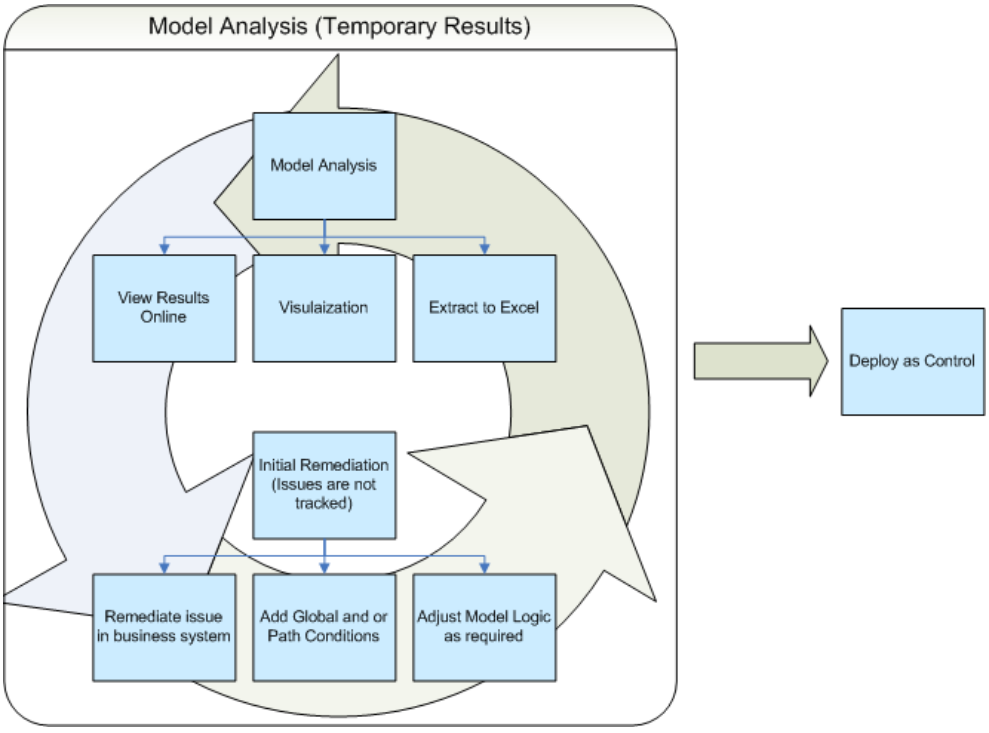
Creating Access Models from Scratch

You may find that you need additional models to meet your company's GRC goals. New models can be created at any time, and can even be copied from existing models where it makes sense to save time.

4

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, you log on to Oracle Application Access Controls Governor and work through these steps to begin analysis in your systems.

☐ **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 results from a model may result in immediate visibility to obvious areas that require remediation in the business system. As a business, you can determine if you require permanent incidents to be generated before any cleanup in the business system happens, or you may choose to do some house cleaning before deploying your model as a control.

In addition, 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. You might want to page through a few to see if any obvious users jump out at you as being obsolete: previous consultants who no longer should have access, employees who are no longer with the company or have switched jobs and should no longer have anything to do with the current model you are viewing conflicting results for, etc.

As you are paging through, you may find that some Application Developer roles are applicable only to the development environment. You might want to use global conditions to exclude these during initial analysis so that you can focus on incidents more likely to appear in your production instance.

You might see a specific role that catches your eye — maybe a super user role. You can enter a filter to limit your model results and focus for a minute on just that role. If that one role has conflicting access points, then you have already identified what is called an "Intra-Role" conflict, meaning in order to remediate that conflict you have to actually 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.

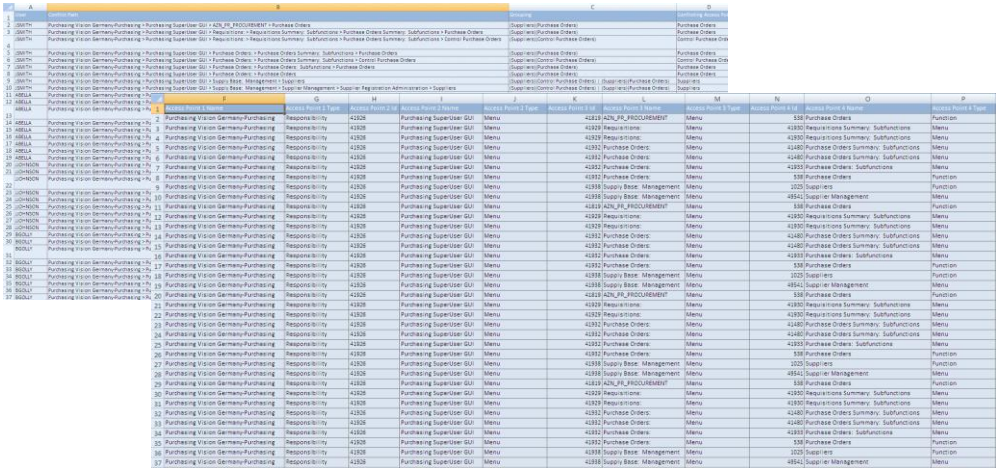
Visualization

In addition to the online view and extracts, Visualization 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 familiar and comfortable using Excel for analysis. Model results can easily be extracted to Excel for further analysis, filtering, charting, pivot tables, etc.

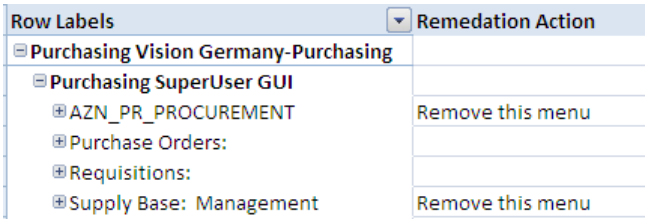
The model results of Access Controls Governor actually break out the access path causing the conflict into individual columns. This allows for very specific analysis within applications like Excel.



For instance I can easily create a pivot of access paths causing conflicts and determine my remediation plan.

In this example, I wanted to further analyze the Purchasing Vision Germany responsibility. I filtered my model results for this responsibility and exported to Excel. The result: thirty-six users violate my model.

To summarize the problem at hand, I can create a pivot table quickly by the individual access point columns and see that my main incident is the Supply Base: Management menu. I also quickly noticed an AZN menu that should be completely removed from the Purchasing SuperUser GUI menu.



Row Labels	Remedation Action
⊟ Purchasing Vision Germany-Purchasing	
⊟ Purchasing SuperUser GUI	
⊞ AZN_PR_PROCUREMENT	Remove this menu
⊞ Purchase Orders:	
⊞ Requisitions:	
⊞ Supply Base: Management	Remove this menu

Initial Remediation

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

Before Deploying a Control

Set Up Tags and Participant Groups

At this point, you are just about ready to deploy your models as controls. Before you do, you will need to do some setups in order to have the options available to you when you create your control. Think about how you want to categorize your controls and who will be involved in the review process when incidents are generated.

Tags assigned to your controls will allow you to filter on those controls (and any incidents generated by those controls) by the tag values you define. For instance, if you have controls handled by certain regions in your company, it may make sense to create a new tag called Region. In that tag 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 a similar control with different conditions focusing on specific operating units that fall within those regions.

Continuing with that example, you would be able to then apply different participant groups 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. Two participant groups could be created and assigned to the appropriate controls.

Specifically for Fusion, instead of the AACG control participants, Fusion uses standard AMX functionality to determine who the appropriate approvers are — this can include organizational hierarchies, multiple mandatory and optional approvers, re-routing, approval delegation, and all other functionality of AMX. In addition, Oracle Identity Management uses the Business Rule Editor to do conditional work-flow evaluations. For instance, Fusion Business Rules may conditionally route SOD conflicts based on the tag values associated to the AACG controls violated. For instance, there may be different people in charge of reviewing incidents for the violations that happen in the North and South American regions versus those in the Europe region.

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 segregation of duty 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 conflict 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.

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.

- Submenu Grant Flag: **N**

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

- 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 item that leads to a function (or access point) included in the control.

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.

- Display Only: **1**

  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: **1**

  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.

Common global-condition exclusions for Fusion are available in the Fusion Access Conditions business object. A best business practice for Fusion has been identified below as a possible condition to set up for analysis exclusions.

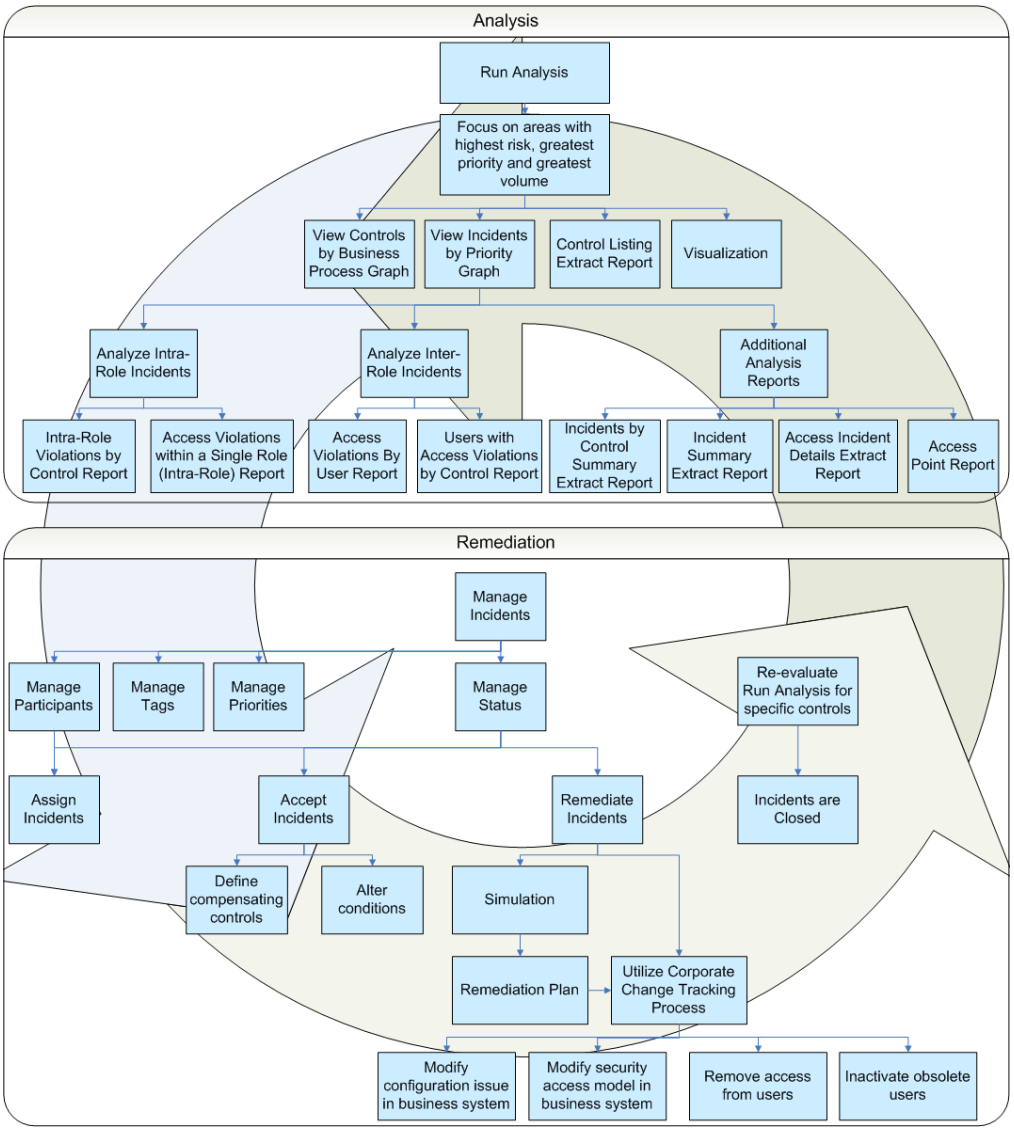
- User Status: **Active**

  Do not apply controls to users that are inactive.

5

Remediation

Remediation is the act of cleaning up your application to reduce or eliminate segregation of duties conflicts defined by controls. A common approach is outlined below.



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 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.)

- ☐ **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.

  Focus next on inter-role incidents. These incidents mean 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, risk, business process and any other tags 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 related 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 various reports and extracts to analyze incidents.

Through Control and Incident Management screens, or via the Report Management task, run various reports to continue analyzing 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 will need to be updated based on various factors and questions such as the following: Who needs to look at this incident? Should we categorize or prioritize this differently? Is this incident acceptable? If so, 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 are the steps outlined in the following section and correspond with the remediation section of the flow chart.

☐ **7** Manage Participants.

Various people should review and act on the incidents that are generated. Generally different business owners are interested when different controls are violated. To help manage these incidents, they are automatically assigned to the participants of a control where "Assign Incident" is set to yes. Existing participants of an incident may choose to reassign or add participants as necessary during the review process.

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 be focusing on cleanup of one user, the removal of a function from a menu may affect many users.

☐ **8** Manage Tags.

Create new tags and tag values to help categorize your controls and incidents in a manner that helps you when filtering, analyzing, and cleaning up incidents. For instance, if it makes sense to analyze incidents by region, you may consider creating a tag called Region and adding the desired values such as North America, South America, and Europe.

☐ **9** Manage Priorities.

When incidents are generated, they are assigned the priority associated to the control that was violated. You may find during analysis 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. It is in the "Assigned" status when initially identified. During the remediation phase, participants of an incident may choose to accept the incident or remediate the incident.

Accepting the incident usually means identifying any compensating controls or adjusting the 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 corporate change-tracking process.

Remediation involves 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 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 participants who know and understand the control and risk — you should have been able to add a priority and any tags 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, you may choose to run analysis only on controls with that tag. 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.)

- The Controls by Business Process graph provides a high-level way to see where the volume is the greatest.
- The Incidents by Priority graph quickly brings focus to the distribution of incidents across your priority ranking.
- Use the Control Listing Extract to create pivots, filter and summarize data in a variety of ways to determine your focus area.
- In addition to the graphs and extracts, Visualization 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 panel, analyze using visualization and various filters 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 tags 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 related. 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.

Assign status to incidents: The Manage Incidents 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 grid. This can be done individually or several at a time. By setting the status here, you can return to the manage incidents 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 ETL and analysis is run the status for those incidents that have been cleaned up will automatically be set to a closed status.

Typically, a single participant 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, participants may be assigned to individual incidents if desired.

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 ETL and analysis is 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 the reports already mentioned, below are additional reports commonly used to help analyze incidents:

- Incident 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 Incidents 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 Incidents 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.

- BIP Templates

  BIP Templates offer additional reports for which you can modify the report layouts to suit your purposes.

Assign Incidents to Business Owners

When a control is violated, all participants with Assign Incident set to yes are assigned to the incidents generated. It may be appropriate to reassign incidents to a business owner who is more directly interested in the incident. When that person logs on to the Manage Incidents screen, she will automatically be viewing 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. As you do, the simulation feature builds a remediation plan, essentially listing, as steps, the child access points and the parents from which they would be removed. Once you are satisfied with your plan, you run 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 to simply 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 Incidents 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, AACG closes the original issues, because the Releases versus Invoice Approve conflicts are resolved. But AACG creates two new issues, at the Assigned status, because the Purchase Orders versus Invoice Approve conflicts remain unresolved.

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)	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)|(Releases)(Invoice Approve)	Closed
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 > AP_INVOICES_GUI12 > AP_INVOICES_ENTRY_GUI12 > AP_APXINWKB_MENU > Invoice Approve	Invoice Approve	(Purchase Orders)(Invoice Approve)	Assigned

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.

6

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 they are being assigned duties in the Oracle FND Users form or the PeopleSoft User Profile page. 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 participants designated by the control. If a reviewer approves, the assignment is allowed; if he rejects, it is disallowed.

In Oracle EBS, Access Approvals 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.

If the control finds conflicts in Oracle Fusion, the review process is handled by Oracle Identity Management; although records of these conflicts appear in the EGRCC Manage Access Approvals page, it's recommended that control participants do nothing with them. (When conflicts are resolved in Oracle Identity Management, their records are removed automatically from the Manage Access Approvals page.)

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

Manage Access Approvals Maintenance

For an initial period after installation, a site may wish to run AACG with the Access Approvals feature turned off, so that 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 EGRCC role that incorporates the Manage Access Approvals permission, assign that role to users, and for those users (or participant groups to which they belong) set the "Assign Incidents" to yes in controls.

To implement Access Approvals in Fusion, see the *Oracle Governance, Risk and Compliance Installation Guide*. Refer to section "Performing GRC Setup in Fusion Setup Manager".

To Turn Manage Access Approvals Off in Oracle

To turn Manage Access Approvals off in an Oracle 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.

To Turn Manage Access Approvals Off in PeopleSoft

During installation of EGRCC, 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 and Upgrade 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*.

To Turn Manage Access Approvals Off in Fusion

For information on turning Manage Access Approvals off (or on) in Fusion, see the *Oracle Fusion Applications Post-Installation Guide, 11g Release 1 (11.1.1.5.0)*, part number E22380-01.

Defining Your Notification Schedules

Notification schedules determine how often users are notified when incidents are generated. For each control participant where Notify is set to yes, a consolidated email message is generated, showing all controls violated, but not yet 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 Data and System Administration chapter of the *EGRCC User Guide*.

7

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 participants of an incident may view and act on an incident. Also by default, only “Pending” incidents (those with a status of Assigned or Remediate) 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 grid.

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 recommend 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 tags 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, participants (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.

A

Appendix: Upgrade Benefits

Version 8.6.3 of Application Access Controls Governor offers many features that are either enhancements of those available in previous versions, or entirely new, as the following table shows:

Feature	7.x	8.5	8.6.x
Next Generate Access Control Engine			
• Cross-Platform (Instance A to Instance B)		×	×
• Multi-Platform (Oracle, PeopleSoft, Other*)		×	×
Access Modeling			
• Create Access Models in Graphical Format			×
• View, filter, extract or visualize temporary results before creating incidents			×
• Centralized Manage Models screen for Transaction and Access			×
Robust Access Control Authoring & Handling:			
• Complex Operand Combinations		×	×
• Entitlements		×	×
• Global Level Conditions	×	×	×
• Control Level Conditions		×	×
• Path Level Conditions		×	×
• Contextual Filtering and Sorting	×	×	×
• Edit multiple records and save once		×	×
• Centralized Manage Controls screen for Transaction and Access			×
Comprehensive Remediation:			
• Centralized Incident Management		×	×
• Contextual Reports	×	×	×
• Embedded BI (graphs, etc.)		×	×
• Full Path Display		×	×
• Graphical Simulation	×	×	×
• Contextual Filtering and Sorting		×	×
• Centralized Manage Incidents screen for Transaction and Access			×

Feature	7.x	8.5	8.6.x
BIP Reporting			
• Customer Organized and Administered Reports		×	×
• Customizable report layouts		×	×
• Seeded Templates		×	×
• Reporting decoupled from product releases		×	×
Flexible User Security (role creation, user assignment)		×	×
Manage Access Approvals			
• Oracle Access Approvals	×	×	×
• PeopleSoft Access Approvals		×	×
• User Request and Administration Screens		×	×
• Consolidated Notifications		×	×
Internationalization		×	×
Job History and Job Scheduling	×	×	×
Purge Incidents		×	×
Visualization		×	×
Participant Groups		×	×
Import/Export			
• UI control selection for Import/Export		×	×
• Datasource mapping of Controls		×	×
Integration Support			
• GRCI Integration		×	×
• OIM Integration		×	×
• ORM Integration		×	×
• OAM Integration		×	×
REST based Web Services		×	×

*Fusion connector is available out-of-the-box in version 8.6.3. Refer to the *Extensibility Framework Guide* for information creating connectors for other business applications.