Application Access Controls Governor Implementation Guide 8.5.1

ORACLE

Application Access Controls Governor Implementation Guide 8.5.1

Primary Author: Stephanie McLaughlin

Contents

Application Access Controls Governor Setup Overview

Oracle Application Access Controls Governor (AACG) is a segregation-of-duties policy-authoring and -handling solution that works across heterogeneous platforms to detect and prevent undesired user access. It runs in a Governance, Risk and Compliance Controls platform, which it shares with another application called Transaction Controls Governor. As you implement AACG, you will use software tools specific to it as well as GRCC software tools common to the two applications.

Each AACG policy specifies “access points” to a company’s business-management applications that should not be assigned simultaneously to individual users. AACG then finds “conflicts” — assignments of duties to business-management-application users that violate access policies.

Because AACG was designed with rapid implementations in mind, best-practice SOD libraries may be used to deploy policies for immediate conflict analysis. The best-practice SOD Library for PeopleSoft and E-Business Suite provides access policies that support rapid implementation of segregation of duties around common end-to-end business processes. These include Order to Cash, Procure to Pay, Financials, and Human Resources.

Consider the guidelines in this chapter as you set up AACG for your organization.

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 include several areas that 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 issues 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 issues 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 GRCC 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 issues.
    b. Search for any patches that may need to be applied.
2. Refer to the *Compatibility Matrix* document for the preferred and supported hardware configurations.

3 Look on Oracle Support for known environment variable issues.

4 Follow the *GRCC Installation and Upgrade Guide* to install GRCC.

5 Verify that areas of the application are working (see the *AACG* and *GRCC User Guides* for more information).

   a Create a datasource and run ETL synchronization.

   b Create a simple access policy to test (for example, Responsibility 1 vs. Responsibility 1, so that the assignment of this responsibility to anyone would cause a conflict).

   c Run conflict analysis.

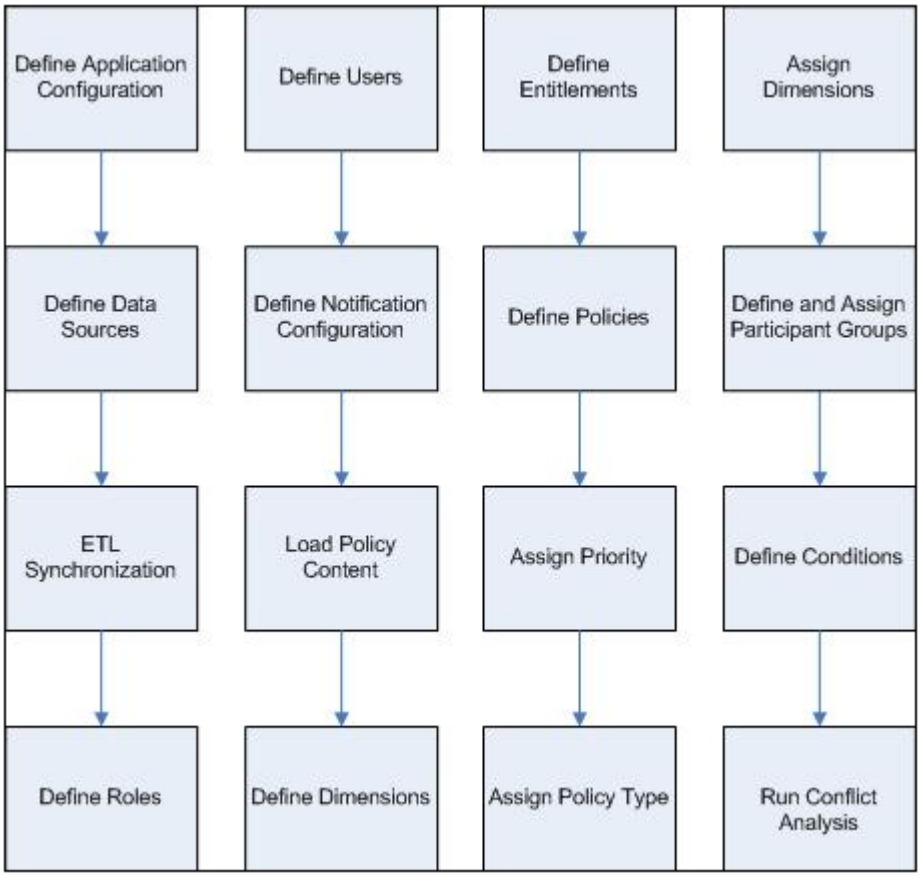
   d View conflict-analysis results.

   e Run a few reports.

6 Continue setups as recommended in this *Implementation Guide*.

Application Access Controls Governor Setup Flowchart

Although you can set up Application Access Controls Governor in many ways, we recommend that you follow the order suggested in the following flowchart. 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 Governance, Risk and Compliance Controls, in which you can find full information about the procedures for completing each step.)

- ☐ 1 **Required:** Connect your instance of GRCC 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 Administration chapter of the *GRCC 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 Integration tab on the GRCC Application Configuration page, you would provide information GRCC uses to connect to the Data Analytics schema.

  See "Setting Properties" in the Data Administration chapter of the *GRCC 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 Administration chapter of the *GRCC User Guide*.

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

  See "Synchronizing Data" in the Data Administration chapter of the *GRCC 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 the nodes you can select in the Navigation panel, generally following its hierarchy, and so assign privileges to work in the screens that can be opened from the Navigation panel.

  GRCC comes with two roles already defined — Basic provides access only to a Home panel, and Admin provides access to all (AACG and TCG) 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 *GRCC User Guide*.

- ☐ 6 **Required:** Define AACG users and grant them roles. GRCC 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 GRCC 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 *GRCC User Guide*.

- ☐ 7 **Optional:** Configure notifications. When a policy generates conflicts, AACG may notify the policy "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.

  See "Configuring Notifications" in the Data Administration chapter of the *GRCC User Guide*.

- ☐ 8 **Optional:** Load policy content. The AACG export, import, and migration utilities capture not only access policies, but also entitlements (see step 10) used by those policies. Best-practice SOD libraries for PeopleSoft and E-Business Suite may be loaded to support rapid implementation of segregation of duties.

  See "Exporting, Importing, and Migrating Policies" in the Creating Access Policies chapter of the *AACG User Guide*.

- ☐ 9 **Optional:** Define dimensions. A dimension is a category of values. Its values may be assigned to access policies (and so to conflicts generated by those policies). Or, its values may be assigned to entitlements (see step 10), and so to conflicts generated by policies that include those entitlements. They flag items, and so distinguish them from unrelated items. They may therefore be used as sort criteria in AACG panels that display policies, entitlements, or conflicts.

  See "Creating Dimensions and Assigning Dimension Values" in the Creating Access Policies chapter of the *AACG User Guide*.

- ☐ 10 **Optional:** Define entitlements. Each is a collection of access points. Typically, those points provide access to related functions, and the entitlement name is a business term that reflects the common functionality. To define conflicts, access policies 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 policy, as well as points included independently of entitlements.

  See "Creating an Entitlement" in the Creating Access Policies chapter of the *AACG User Guide*.

- ☐ 11 **Required:** Define access policies (or edit those loaded in step 8). An access policy may define conflicts among any number of access points or entitlements. A single policy 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 conflicts in Oracle E-Business Suite and PeopleSoft Enterprise. It may include both access points and entitlements.

See “Adding an Access Policy” and “Adding Access Points or Entitlements to a Policy” in the Creating Access Policies chapter of the *AACG User Guide*.

☐ 12 **Optional:** Prioritize policies. Assign number values to policies to identify which are most important. When prioritizing, 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 “Adding an Access Policy” in the Creating Access Policies chapter of the *AACG User Guide*.

☐ 13 **Required:** Set policy types. Each access policy is assigned one of three policy types, which determine the actions to be taken when a business management-application user is assigned duties that a policy defines as conflicting:

- A Prevent policy should deny access to conflicting access points. All paths to such a conflict are assigned a Prevent status, and this status cannot be changed.
- A Monitor policy permits access to conflicting access points. Although automated or manual controls may be in place to mitigate conflicts generated by Monitor policies, this is not necessary. Paths to conflicts generated by a Monitor policy are initially set to a Monitor status, indicating that the access should be re-examined periodically. Analysts can update the status to Approved (the user retains access granted by that path, and it need not be re-examined) or Rejected (the user must not have the access granted by that path). Ultimately, the intended choice for a policy of this type is Approved or Rejected.
- An Approval Required policy allows a user to work at conflicting access points only upon approval by a reviewer designated by the policy. Paths to conflicts generated by an Approval Required policy are initially set to a Pending status, and analysts may reset the status to Approved or Rejected.

See “Adding an Access Policy” in the Creating Access Policies chapter of the *AACG User Guide*.

☐ 14 **Optional:** Assign dimensions to categorize policies. As you create policies or entitlements, you can assign dimension values to them. There are two seeded dimensions, Business Process and Risk. By assigning dimension values to your policies, 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 “Creating Dimensions and Assigning Dimension Values” in the Creating Access Policies chapter of the *AACG User Guide*.

☐ 15 **Optional:** Assign “participants” to policies; create “participant groups” for that purpose. Each policy must have at least one participant (individual or group), identified as “first to act.” This participant resolves policy conflicts.

If access points are assigned to an Oracle EBS or PeopleSoft Financials user after an Approval Required policy has been written to define them as conflicting, a record of the assignment appears in the AACG User Provisioning panel. In this case, if the first-to-act participant is an individual, he has exclusive re-

sponsibility for reviewing the assignment; if the first-to-act participant is a group, any member may review the request, but the first to do so acts for all.

Otherwise — if conflicts are generated in other applications, or even within Oracle or PeopleSoft by a Prevent or Monitor policy, or if access points had been assigned to users before the policy was written to define them as conflicting — records of conflicts appear in the Work Queue. If the first-to-act participant is an individual, she is the owner of these records; if the first-to-act participant is a group, a member identified as "primary" is the default owner of these records.

If you do not select a participant for a policy, AACG appoints the admin user as its first-to-act participant.

See "Designating Policy Participants" in the Creating Access Policies chapter of the *AACG User Guide*.

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

- As you create or edit an access policy, you can create conditions for it. These can specify users or other objects, such as companies in PeopleSoft or operating units in Oracle EBS, that are exempt from the policy. Or they can specify circumstances under which the policy 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 the conditions that are configured to apply to an individual policy, except that a global condition applies to all policies 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 menu or a responsibility. A path including those points would be excluded from conflict generation. If, for example, a global path condition excluded function-1 from responsibility-1, an access policy set function-1 in conflict with function-2, and a user had access to both functions, no conflict would occur if the user's access to function-1 came from responsibility-1.
- Add comments to conditions as needed to provide an explanation for the exclusion.

See "Defining Conditions" in the Creating Access Policies chapter of the *AACG User Guide*.

☐ 17 **Required:** Find the conflicts that your access policies define. A Find Conflicts program can evaluate all policies or a selection of them, and can be run immediately or be scheduled to run in the future. (Consider whether to synchronize data first — see step 4 — to ensure that business-management-system data is current and conflict generation is up to date.)

See "Finding Conflicts" in the Finding and Resolving Conflicts chapter of the *AACG User Guide*.

Configuration Planning and Installation

You need to create and set up one or more datasources in the GRCC Data Administrator. 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 "Setup Overview." There are references to other sections of this guide for more detailed instructions.

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

Defining Your Datasources

Before you begin setting up your datasources, consider your environment and your goals. Do you run conflict analysis against multiple applications? For instance, do you connect to one application for Financials and another for Human Resources? Are these on the same platform? Will you analyze conflicts across multiple platforms or even cross-platform? By carefully evaluating your business needs, you can create the necessary datasources so that when policies are loaded or created, they will be able to run against the appropriate datasources.

Defining Your Roles

Before you begin setting up your roles, consider who will use AACG (and GRCC), 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 dimensions, review/create policies, and run reports.
- Business Area/Application Owners – May conduct activities such as creating policies, creating entitlements, viewing conflicts, updating conflict statuses, and simulating the resolution of conflicts.
- System Administrator – May set up datasources, application configuration, and notification configurations.
- User Provisioning Participants — May review access requests in the User Provisioning 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 policy has been written to define them as conflicting). According to accepted practice, a user who creates policies should not be able to review the conflicts they generate. Therefore the User Provisioning Participant role typically should not also permit users to create access policies.

Defining Your Users

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

Defining Your Notification Schedules

Notification schedules determine how often users are notified when conflicts are generated. For each policy participant, a consolidated email message is generated, showing all conflict paths generated for the participant, but not yet sent. Before creating a notification schedule, consider how often conflicts will be generated, and how immediate is the need to review or fix those conflicts.

ETL Synchronization

To maximize performance and handle cross-platform analysis, application access security model data is extracted and loaded into GRCC 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 ETL synchronization should occur before conflict 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 ETL synchronization on a daily basis.

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

Policy Planning and Setup

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

Defining 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 first to identify policies to be activated, and then focus on the entitlements within those policies for completeness.

Defining Policies

If you decided to load the best-practice SOD library, you will have a number of policies that already identify sets of access points to which individual users should not be granted access.

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 policy and its access points is necessary to ensure that the goals of the company are being met. There are several ways to approach defining policies. 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 policies.

4 Create and edit policies and entitlements as needed.

5 Prioritize policies.

6 Assign policy types.

7 Define and assign dimensions to categorize policies.

8 Assign policy participants.

Defining Conditions

Conditions help eliminate false positives and create focused conflict-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 conflict analysis? This determines what conditions should be set and at what level (global, policy, or path). For instance, certain users (like developers) may cause hundreds of conflicts 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.

Best business practices for Oracle EBS have been identified below as possible conditions to set up for analysis exclusions.

Note: If conditions are not visible, go to Data Administration and click Refresh.

Common global-condition settings for Oracle E-Business Suite are as follows:

- Submenu Grant Flag: **N**

  Do not apply policies 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.)

- Query Only: **QUERY_ONLY**

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

- Function Grant Flag: **N**

  Do not apply access policies 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: **Inactive**

  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: **Inactive**

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

- User Responsibility End Date: **Inactive**

  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.

- Prompt: **No Prompt**

  Policy violations are excluded if there is no prompt for a menu item that leads to a function (or access point) included in the policy.

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 provided. 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 issues 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.

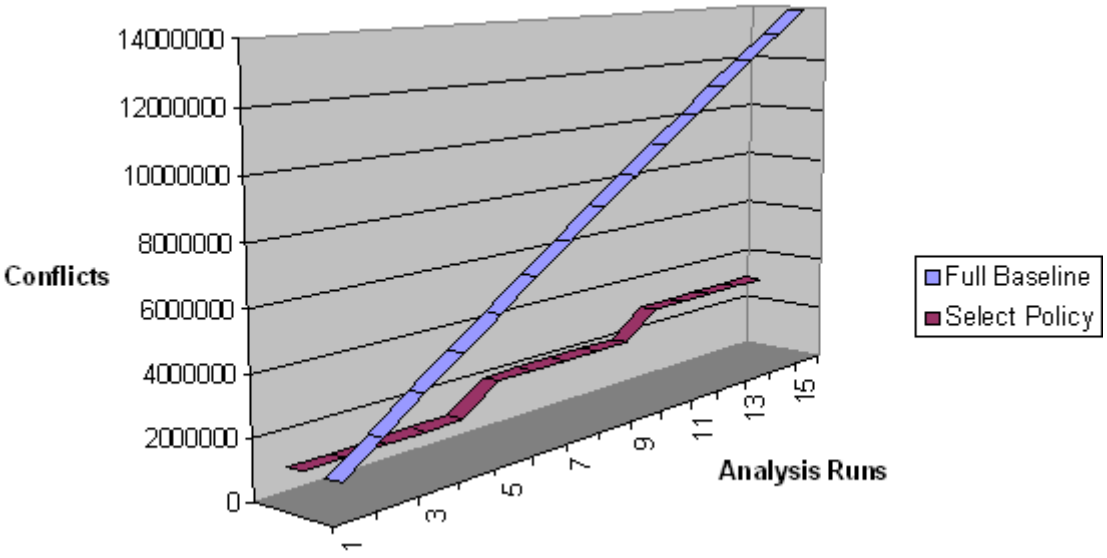
Establishing and Using Baselines

A common mistake that users perform is to run the Conflict Analysis process for *all* of their active policies every time or on a frequent basis. What this does is recreate each conflict (and related conflict paths) over and over for each run. So if you have a million conflicts for all of your policies, you generate a million new rows each time you perform a new run. This is because AACG stores each conflict, and related paths, by run so that remediation performance metrics can be provided from one run to another and can be used to show the progress made over time.

Adding a million new rows per conflict run may not sound like a lot, but considering that each conflict can have multiple conflict paths, managing how many conflicts you generate is important. Each conflict path is a set of data that must be reviewed and analyzed each time there is a conflict analysis run, as each path is considered to be a potentially new conflict unless it is matched with an existing conflict path. This prevents the creation of duplicate violations each time there is a conflict analysis run.

Example: An organization has 1 million conflicts to begin with. If the organization performs full baseline runs each time and removes 10,000 conflicts each analysis run, over 15 runs the number of conflicts that have been generated is approximately 14 million. Over that same number of runs, if a full baseline is run only every fifth run, analysis is

done only on select policies with 10,000 conflicts each and with the same rate of conflict removal as in the full baseline, the number of conflicts generated is approximately 3.9 million. The difference is illustrated in the following graph:



Being able to see all the conflicts that exist at a given time is a good thing, as it establishes a baseline against which you can measure progress, and scope the initial and remaining work to be performed. However, after the baseline is established the actual work of removing the existing conflicts should be done one policy at a time.

The rationale for this approach is two-fold. First, as previously mentioned, the number of overall conflicts that must be processed is significantly smaller. Second, users will approach the removal of conflicts one policy at a time. So, having all the extraneous data incurred with a full baseline analysis run provides no value at all.

Best practice in remediating conflicts starts with a user force ranking their policies by order of priority and/or volume of conflicts. Subsequent runs should be orchestrated to systematically work through the policies individually. The conflict analysis runs will be much quicker since inherently the volume is significantly less for one policy than it is for all. Periodically, as deemed necessary, you can generate full baseline runs (most likely over a weekend at this stage) to get a feel for the overall progress that is being made.

Remediating Conflicts

Simply identifying SOD violations that exist is not the intent of AACG. Rather the removal of the conflicts as a remediation option is considered best practice. Procedurally you can increase performance just by removing the volume of data (conflicts and conflict paths) being generated.

Begin remediating the roles with the largest conflict results within the prioritized policies. Reviewing the design of the responsibilities themselves and removing as many intra-role conflicts as possible will significantly reduce the number of conflicts and related conflict paths, and inherently the performance will increase proportionately. Every time a single

responsibility containing multiple conflicts within its design is assigned to a user, all those conflicts are being repeated. Considering that, its easy to see how this is the logical first place to start in the remediation process.

After the high volume intra-role conflicts are removed, the remaining conflicts for the policy should be addressed. This may be done by also fixing the design of certain roles, removing access that grants extraneous access, or by removing the provisioning of the roles themselves.

In addition to the remediation steps outlined above, some versions of Oracle generate many conflict paths because of “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)

As you progressively clean up the SOD violations that exist in your environment, the application will be perform more efficiently.

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 policy compares one entitlement with another, the end result is basically the cross-product of those entitlements. That is, the policy consists of “subpolicies,” 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
- Assign Flexfield Security Rules
- Assign Key Flexfield Security Rules
- Suspense Accounts
- Consolidation Mapping Sets
- Elimination Sets
- Subsidiaries
- Define Transformation Rules
- Define Elimination Formulas
- AutoPost Criteria
- Journal Categories
- Journal Authorization Limits
- Submission Schedules
- Journal Sources
- Statistical Units of Measure
- Cross-Validation Rules
- Assign Descriptive Flexfield Security Rules
- Summary Accounts
- Consolidation Mappings
- Purge Consolidation Audit Data
- GIS AutoAccounting Rules
- Intercompany Transaction Types
- Financial Item
- Account Hierarchy Editor
- Reversal Criteria
- Concurrent Program Controls
- Encumbrance Types
- Storage Parameters
- Tax Options

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 setup a policy that compared these entitlements — say, General Ledger Setup vs. Process GL Transactions — we would in essence have a total of 1,450 subpolicies. 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 policies are broken down and more specific, priorities and dimensions can be assigned so the most import areas are focused on first.
- There is no way to focus on specific conflicts to analyze and finally remediate since it has all been grouped as one large policy.

- Voluminous amounts of data would be returned each time conflict analysis is run for the policy. In general, analysis and remediation is going to happen iteratively, there is no reason to continually generate conflict paths when no remediation effort has even taken place.

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

Security Rule Definitions

AP Accounting Flexfield Combinations GUI	Cross-Validation Rules
Assign Flexfield Security Rules	Assign Descriptive Flexfield Security 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 policies — Manage Journals vs Security Rule Definitions and Manage Journals vs Open and Close Periods.

Generally, entitlements will have between five and ten access points that group together very like functionality. (Note: It is a good idea to create 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 policies.)

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

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

On top of these benefits, having focused policies to run conflict analysis against and take action in an iterative process will keep the volume of transactions generated to a minimum. This will not only help performance while accessing various screens and running reports (because there is less data to sift through), it will also save on storage space.

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

AND
    Manage Journals

OR
    Security Rule Definitions
    Open and Close Periods

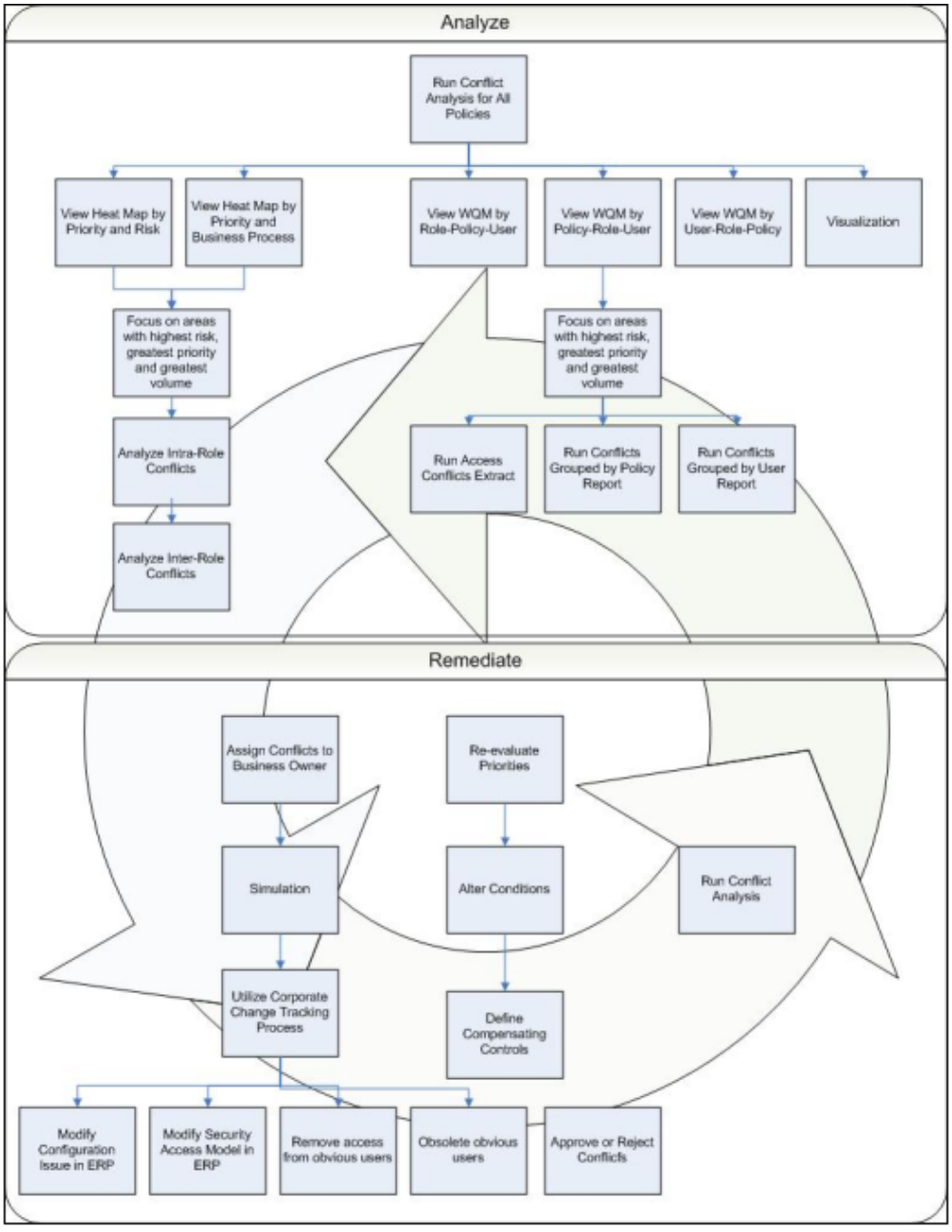
Following these suggestions should provide the most optimal AACG experience.

Remediation

Remediation is the act of cleaning up your application to reduce or eliminate segregation of duties conflicts. Segregation of duties simply means that each user should not be assigned access points that policies define as conflicting in a system (or systems). Although there may be similarities, segregation of duties is different for every company, and the process for cleaning up the conflicts that may occur is also different.

Outlined below is a common approach to remediation. It may need to be adjusted based on your company's goals for Governance, Risk, and Compliance.

Remediation Flowchart



Remediation Considerations

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.

Remediation Checklist

The following checklist provides a more detailed list of steps using Application Access Controls Governor during 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 conflict analysis for *all* policies.

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

☐ 2 View the Heat Map in various ways.

Use the Heat Map to select various combinations of the X and Y axes to provide high-level counts of conflicts in your system. This will help determine the best area to begin focusing on conflict analysis and remediation.

☐ 3 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 user, or policy, or any other category that produces a large number of conflicts.) The Heat Map provides a high-level way to see where the volume is the greatest. Use the Heat Map to continue drilling into more layers of data, or move into more detailed data via online screens and reports.

If an initial analysis run returned a high volume of conflicts, you should not only decide on a focus area, but also inactivate policies that don't contribute conflicts to that focus area. (For example, if you choose to focus on policies, select one or two with the greatest number of conflicts, and inactivate the rest.) Keep in mind that each time conflict analysis is run, AACG stores a record of the conflicts it finds. Storage and queries will obviously be affected by this; therefore focusing on selected areas is recommended.

☐ 4 Review intra-role conflicts.

Focusing on intra-role conflicts first will inherently clean up potentially hundreds of conflicts. (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 issues and cleaning them up first, you will see an across-the-board effect.

☐ 5 Review inter-role conflicts.

Focus next on inter-role conflicts. These conflicts 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 conflicts.

☐ 6 Use various on-line views to analyze conflicts.

In the AACG Work Queue, various on-line views group and summarize data at a high level; you can drill into each view for more detailed analysis. Try running the different Work Queue views to determine more accurately where your conflicts reside.

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

☐ 7 Use various reports and extracts to analyze conflicts.

Through the Conflict Analysis screen, or the Conflict Reports area of the Report Center, run various reports to continue analyzing data. Use the Conflict Access Extract to evaluate data in Excel and create necessary filters and pivot tables to analyze the data.

☐ 8 Assign conflicts to business owners.

Various people should review and act on the conflicts that are generated. Generally different business owners are interested when different policies are violated. To help manage these conflicts, paths should be assigned or claimed so that they will show up in the appropriate person's Work Queue to be acted on (approved, rejected, or monitored).

Note, though, that as the cleanup process continues, many conflicts identified in the early rounds of analysis will disappear from the Work Queue as your remediation steps resolve them. So, in the earlier rounds, you may choose to make limited use of the Work Queue — use it to view conflict paths, but not actually assign status to them or send notifications to policy participants. You could begin to make full use of the Work Queue when cleanup is mostly complete.

☐ 9 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.

☐ 10 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.

☐ 11 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 conflicts on the next run.

☐ 12 Re-evaluate.

A common approach to remediation is to analyze conflicts, prioritize them, add focus with conditions, clean them up, and then re-evaluate. Initial remediation may require new conflict 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 conflict analysis run at the end of each week to provide a fresh look at where conflicts 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 Conflict Analysis for *All* Policies

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

When loaded, all entitlements are active. However, policies are loaded as inactive. Use the Mass Edit feature to update all policies to Active. If there are polices that obviously do not make sense to your business, you may want to leave those as inactive. However, it doesn't hurt just to activate all policies, as they can be easily inactivated later if desired.

Your current knowledge of the company's GRC goals and priorities will determine your next steps. In some cases, you might want to run conflict analysis at this point, before assigning priorities or dimension values. If you already have a general idea and want to update policies with priorities and dimension values, it will give you more ways to view the data in the Heat Map, online screens, and reports.

Run the Find Conflicts > Run Now program from the Policy Definition Screen when you are ready to run conflict analysis.

See "Exporting, Importing and Migrating Policies" and "Editing an Access Policy" in the Creating Access Policies chapter, and "Finding Conflicts" in the Finding and Resolving Conflicts chapter, of the *User Guide.*

View the Heat Map in Various Ways

Use the Heat Map to select various combinations of the X and Y axes to provide high-level counts of conflicts in your system. This will help determine the best area to begin focusing on conflict analysis and remediation.

The Heat Map enables analysts to prioritize the resolution of conflicts by determining where the greatest numbers are being generated. It sorts conflicts according to user-selected parameters, and displays the results graphically. The analyst selects two parameters to produce an initial sort. She then chooses one set of the conflicts returned by that sorting and applies an additional parameter to it, to focus results more narrowly. She may repeat this process, producing still more finely focused results.

From the Home page, select Priority and Business Process as the initial parameters, and then click Go. This gives you counts. Generally, focus on the business process that has the highest volume with priority 1. At this point, you would most likely want to see which roles are affected so that you can begin to focus on cleaning up those roles. Select Role from the drill down and click on the cell in the heat map that you want to drill into.

See “Using the Heat Map” in the Finding and Resolving Conflicts chapter of the *User Guide*.

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

The Heat Map should have given you a pretty good idea of where your biggest areas of concern are. There are various ways to continue analyzing the data. Below we will go through some examples.

Review Intra-Role Conflicts

Intra-Role Conflicts 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 conflicts, you may also clean up several inter-role conflicts.

1. View the Heap Map; select Priority and Role as your initial parameters. This shows which role with the highest priority has the greatest number of conflicts.
2. Drill into Role to view Policies. In the Drill Down Menu, select Bar Graph and Policy. Then click on the cell for the priority and role with the greatest number of conflicts.
3. View Policies. This shows all the policies that have been violated by the role and priority you selected.
4. Try to determine intra-role conflicts. In the Drill Down Menu, select Work Queue and User. Then, in the bar graph, click on the bar for a policy. This opens the Work Queue, where you can see the users who violate the policy you selected. Select various users to view the access points involved in the policy violation — the access points that conflict with one another should become apparent. Also try using the Visualization feature to view the conflict paths in a graphical format.
5. Determine how to remediate.

   From Display, select List. This brings you into the Conflict Analysis screen and shows a list of all conflict paths being violated, still filtered from your drill down.

   Expand the Path column to search for commonality among the paths. For instance, to clean up an intra-role conflict, you would need to remove one or more of the access points that conflict with the other access points. You may find that an access point

must be removed, that paths containing it have a menu in common, and so by removing that menu you could resolve the intra-role conflicts.

6 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, policies and users. See “Simulation” in the Finding and Resolving Conflicts chapter of the *User Guide*.

7 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.

8 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 Conflicts

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

1 View the Heap Map; select Priority and Policy as your initial parameters. This shows which policy with the highest priority has the greatest number of conflicts.

2 Drill into User to view Policies. In the Drill Down Menu, select Bar Graph and User. Then click on the cell for the priority and policy with the greatest number of conflicts.

3 View Users. This shows all the users with violations of the policy you selected.

4 Try to determine inter-role conflicts. In the Drill Down Menu, select Work Queue. In the bar graph, click on the bar for a user. This opens the Work Queue, where you can see the policy violations for the user you selected. The access points that conflict with one another across roles should become apparent. Generally, these conflicts are caused by a user having more roles than he or she requires. Also try using the Visualization feature to view the conflict paths in a graphical format.

5 Determine how to remediate.

From the Work Queue, you may be able immediately to see roles that should be removed from the user. You may want to do further analysis, possible in the Conflict Analysis screen.

From Display, select List. This brings you into the Conflict Analysis screen and shows a list of all conflict paths being violated, still filtered from your drill down.

Expand the Path column to search for commonality among the paths. For instance, to clean up an inter-role conflict, you would need to see where one set of access points have another set of conflicting access points in a different role.

You may need to clean up a menu structure, or possibly just remove a role from a user to remediate the conflicts.

6 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, policies and users. See “Simulation” in the Finding and Resolving Conflicts chapter of the *User Guide*.

7 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.

8 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 Conflicts

The Work Queue screen has three common ways to view and begin remediating conflicts. A general approach to remediation is to begin looking at conflicts in the following order:

- Role-Policy-User

  Use the Role-Policy-User display to see, at a quick glance, the roles with the most conflicts in your system. Within each role, see the policies and the number of conflicts for each. From here you can see the users who violate the policy and determine the best method of remediation.

- Policy-Role-User

  Use the Policy-Role-User display to see, at a quick glance, the policies with the most conflicts in your system. Within each policy, see the roles and the number of conflicts for each. From here you can see the users who violate at that role and determine the best method of remediation.

- User-Role-Policy

  Use the User-Role-Policy display to see, at a quick glance, the users with the most conflicts in your system. For each user, see the roles and number of conflicts at each. From here you can see the policies the user has violated and determine the best method of remediation.

Use the Work Queue: From the Work Queue, you can select a “View” panel, which lists all conflict paths that have not been assigned to reviewers, and either assign them to others or claim them for yourself. You can then open a “My Queue” panel, which lists the conflict paths that you have claimed or that have been assigned to you by others, and select statuses for them.

Typically, a single user would be assigned (or would claim) all the paths to a given conflict, so that the entire conflict can be addressed in a coherent way. However, for

enhanced flexibility, reviewers are assigned to individual conflict paths, so multiple reviewers can address facets of an individual conflict.

Assign status to conflicts: The Work Queue has functionality to set statuses on each conflict path. For instance, if a policy has been set with the Approval Requited policy type, the conflicts it generates can be set to Approved or Required in the Work Queue. By setting a value here, you can return to the Work Queue later to review rejected conflicts and decide how to remediate, or you can run reports for rejected conflict paths and determine how to clean up your business system.

During initial remediation, instead of setting statuses, you will want to use your corporate change-tracking system to remediate changes in the business system and re-run conflict analysis. During this iterative process, conflicts will begin to dwindle.

When conflicts are at a manageable volume, you may choose to begin using the Work Queue to assign statuses. For instance, you may want to "approve" conflict paths if you do not plan to remediate them, but want to show your auditors that you are aware of them and have noted how you are mitigating them.

See "Assigning Status in the Work Queue" in the Finding and Resolving Conflicts chapter of the *User Guide*.

Use Various Reports and Extracts to Analyze Conflicts

Running a seeded conflict report or extract is another way to analyze conflicts and help with remediation. Below are reports commonly used to help analyze conflicts:

High-level summary type reports:

- The Intra-Role Violations by Policy lists policies that generate conflicts involving privileges granted within a single role.
- The Users with Access Violations by Policy access policies that have generated conflicts. For each policy, it lists users whose work assignments have violated the policy. For each user, the report supplies both the global user ID and the user's full name.

Detail type reports:

- Access Violations within a Single Role (Intra-Role)

  A common way to use this report is to solve for intra-role conflicts. First, use the Heat Map to understand where your highest priority and risks have identified the greatest volume of conflicts by Role. Then run this report and focus on cleaning up those high-risk roles 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" policy — 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.

- Access Violations by User

  A common way to use this report is to solve for inter-role conflicts. First, use the Heat Map to understand where your highest priority and risks have identified the greatest volume of conflicts by policy. Then run this report for that policy. By doing so, you will get a list of users that have violated that policy, and be able to quickly see who has access to more than one role causing conflicts.

- 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.

- Access Conflicts Extract Report

  The ability to extract data from the Conflict Analysis screen is for using pivots and filters to slice and dice data in a variety of ways. Generally, you start with the Heat Map to understand where you should focus. Once you've determined the area on which you want to focus for remediation (i.e., Policies, Roles, Risks, Business Areas, Users or a combination of these), go to the Conflict Analysis screen and enter your filter to view the data to extract. Then select Report > Access Conflicts 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 issues.

- BIP Templates

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

See the Reporting chapter of the *Application Access Controls Governor User Guide*.

Assign Conflicts to Business Owners

When a policy is created, a first-to-act participant is assigned to it. When it generates conflicts, their paths are assigned to this participant (or, if the participant is a group, its "primary" member). It may be appropriate to reassign conflict paths to a business owner who is more directly interested in the conflict. When that person logs on to the Work Queue, she may select My Queue to view all the conflicts assigned to her.

Run Simulation

To aid in cleanup, Application Access Controls Governor enables you to simulate graphically how conflict 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 conflicts, roles, policies, 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 "Simulation" in the Finding and Resolving Conflicts chapter of the *AACG User Guide*.

Recommended Use of Simulation

1. Analyze conflicts in the Conflict Analysis page, Visualization, and/or various reports.
2. Determine a "child" access point you would like to remove from a "parent" access point.
3. Create a simulation to see how this would impact your conflicts:
   - 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 the last conflict run. 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 conflicts.

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 conflicts would that impact?
  - What role conflicts would that impact?
  - What policies 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 conflicts?
- 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 “re-drawing” 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

The act of remediation is to make actual changes in the underlying system in which conflicts exist. Options for remediation may be different 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 it is a system administrator type person who will be making 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 rout to remove the desired 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. Conflict 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 conflict.

Re-evaluate

A common approach to remediation is to analyze conflicts, prioritize, add focus with conditions, clean up, and re-evaluate. It is an iterative process. Initial remediation may require new conflict 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 conflict analysis run at the end of each week to provide a fresh look at where conflicts stand. Conflict analysis and remediation are slightly different for every company. This document was intended to provide guidelines and example approaches based on best practices.

User Provisioning

Once most cleanup has taken place, and the customer feels comfortable with the conflicts that are know to remain, the AACG User Provisioning feature is normally turned on. This feature implements “preventive” conflict analysis — it applies access policies 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 policy, and accepts assignments that violate a Monitor policy (or no policy). If an assignment violates an Approval Required policy, AACG suspends the assignment and displays an entry for it in a User Provisioning Requests panel, for review by the first-to-act participant designated by the policy. If that reviewer approves, the assignment is allowed; if he rejects, it is disallowed.

In Oracle EBS, User Provisioning applies only to access granted in the Oracle FND Users form. In PeopleSoft, it applies only to Financials.

See “User Provisioning” in the Finding and Resolving Conflicts chapter of the *AACG User Guide*.

User Provisioning Maintenance

For an initial period after installation, a site may wish to run AACG with the User Provisioning feature turned off, so that conflicts that existed prior to the installation of AACG can be cleaned up before new conflicts are addressed. (Moreover, User Provisioning is typically run in a production instance, but not in a test instance.) Thus, it is possible to turn User Provisioning 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 User Provisioning (as already noted; see page 7), you must not only turn it on, but also create at least one GRCC role that incorporates the User Provisioning property, assign that role to users, and specify those users (or participant groups to which they belong) as first-to-act participants in policies.

To Turn User Provisioning Off in Oracle:

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 User Provisioning 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, User Provisioning requests are stored; when communications resume, a User Provisioning Request Recovery concurrent program sends the stored requests to AACG. It takes no parameters, and is typically scheduled to run periodically.

To Turn User Provisioning Off in PeopleSoft:

During installation of GRCC, a "Provisioning Embedded 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 User Provisioning is running in the PeopleSoft instance) was set to the value *y*.

To turn user provisioning off, you must, in essence, reinstall the PeopleSoft Provisioning 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 User Provisioning back on, reinstall the Provisioning Embedded Agent once again, with the "Enable PeopleSoft PEA" property reset to the value *y*.

Appendix: Upgrade Benefits

Version 8.5 of Application Access Controls Governor offers many features that are either enhancements of those available in version 7.*x*, or entirely new, as the following table shows:

Feature	7.x	8.5
Next Generation Access Policy Engine:		
• Cross-Platform (Instance A to Instance B)		×
• Multi-Platform (Oracle, PeopleSoft, Other*)		×
Robust Access Policy Authoring & Handling:		
• Complex Operand Combinations		×
• Entitlements		×
• Global Level Conditions	×	×
• Policy Level Conditions		×
• Path Level Conditions		×
• Contextual Filtering and Sorting	×	×
• Edit multiple records and save once		×
Comprehensive Remediation:		
• Centralized Work Queue Management		×
• Contextual Reports	×	×
• Embedded BI (Heatmaps, etc.)		×
• Full Path Display		×
• Graphical Simulation	×	×
• Contextual Filtering and Sorting		×
BIP Reporting		
• Customer Organized and Administered Reports		×
• Customizable report layouts		×
• Seeded Templates		×
• Reporting decoupled from product releases		×
Flexible User Security (role creation, user assignment)		×
User Provisioning		
• Oracle User Provisioning	×	×
• PeopleSoft User Provisioning		×
• User Request and Administration Screens		×
• Consolidated Notifications		×
Internationalization		×
Job History and Job Scheduling	×	×
Purge Conflict Analysis Runs		×
Visualization		×
Participant Groups		×

(Table continues on next page.)

Feature	7.x	8.5
Import/Export		
• UI policy selection for Import/Export		×
• Datasource mapping of Policies		×
Integration Support		
• GRCI Integration		×
• OIM Integration		×
• ORM Integration		×
• OAM Integration		×
REST based Web Services		×