Application Access Controls Governor Implementation Guide 8.2.1

ORACLE

Application Access Controls Governor Implementation Guide 8.2.1

Primary Author: Stephanie McLaughlin

Contents

Application Access Controls Governor Setup Overview 1
Diagnostic Steps 1
Application Access Controls Governor Setup Flowchart 2
Setup Checklist 3
Configuration Planning and Installation 7
Defining Your Data Sources 7
Defining Your Roles 7
Defining Your Users 8
Defining Your Notification Schedules 8
ETL Synchronization 8
Policy Planning and Setup 9
Defining Entitlements 9
Defining Policies 9
Defining Conditions 9
Remediation 11
Remediation Flowchart 11
Remediation Considerations 12
Remediation Checklist 12
Application Access Controls Governor Remediation Steps 14
Run Conflict Analysis for *All* Policies 14
View the Heat Map in Various Ways 14
Focus on Areas with the Highest Risk, Priority, and Volume 15
Review Intra-Role Conflicts 15
Review Inter-Role Conflicts 16
Use Various On-Line Views to Analyze Conflicts 17
Use Various Reports and Extracts to Analyze Conflicts 18
Assign Conflicts to Business Owners 19
Run Simulation 19
Utilize Corporate Change-Tracking Process 20
Make Changes in the Underlying System 20
Re-evaluate 20
User Provisioning 21
User Provisioning Maintenance 21
To Turn User Provisioning Off in Oracle: 21
To Turn User Provisioning Off in PeopleSoft: 22

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. Each 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 *Hardware Platform Requirement* 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 of AACG.

It is highly recommended during implementation planning that sufficient time be allocated for setting up, testing, and troubleshooting environment-specific issues that commonly occur 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 AACG 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 *Hardware Platform Requirement* document for the preferred and supported hardware configurations.
3. Look on Oracle Support for known environment variable issues.
4. Follow the *Installation and Upgrade Guide* to install AACG.

5 Verify that areas of the application are working (see the *User Guide* for more information.

   a Create a data source 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.

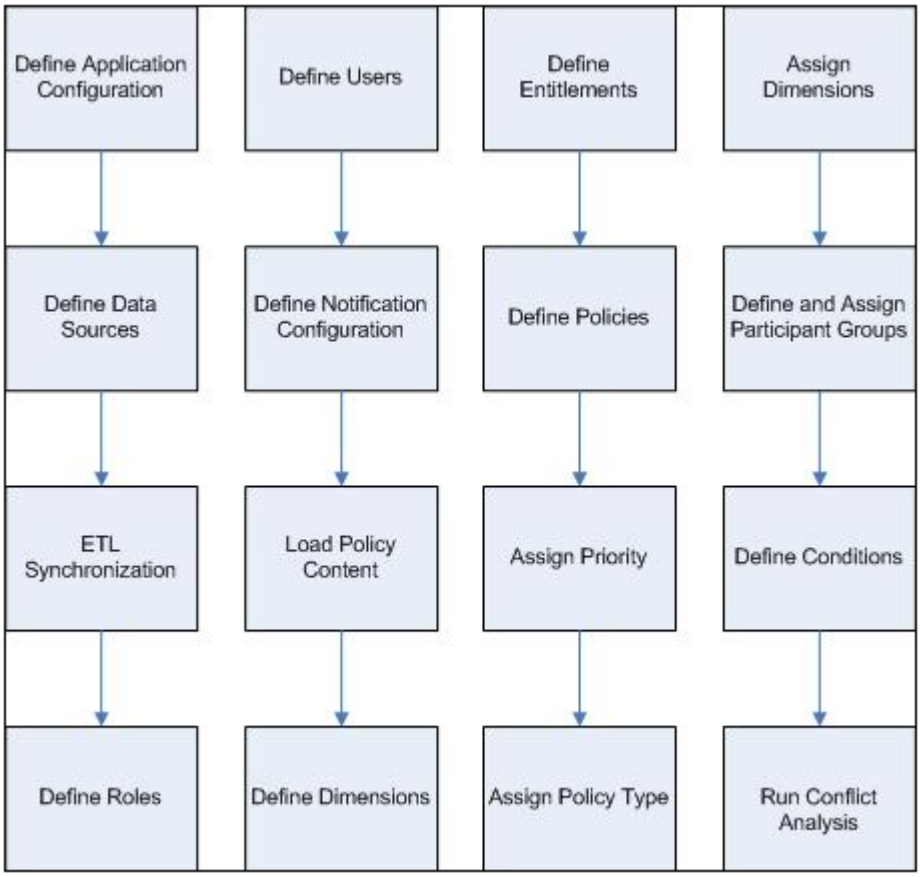
   d View conflict-analysis results.

   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 *Application Access Controls Governor User Guide*, in which you can find full information about the procedures for completing each step.)

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

  See "Setting AACG Properties" in the Data Administration chapter.

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

  See "Configuring a Data Source Connection" in the Data Administration chapter.

- ☐ 3 **Required:** Run "synchronization" to consume the access security model for each data source.

  See "Synchronizing Data" in the Data Administration chapter.

- ☐ 4 **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.

  AACG comes with two roles already defined — Basic provides access only to a Home panel, and Admin provides access to all features other than a User Provisioning panel. User Provisioning provides "preventive" conflict analysis in Oracle EBS instances; typically it is not implemented until conflicts already existing in business-management applications are cleaned up. Thus role creation is optional because you may use the existing Admin role to grant access to all the features you will need initially. To implement User Provisioning, however, you must create a new role and select the User Provisioning property for it.

  See "Creating Roles" in the User and Role Administration chapter.

- ☐ 5 **Required:** Define AACG users and grant them roles. Application Access Controls Governor 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 AACG features other than User Provisioning. 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.

☐ 6 **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.

☐ 7 **Optional:** Load policy content. The AACG export, import, and migration utilities capture not only access policies, but also entitlements (see step 9) 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.

☐ 8 **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 9), 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.

☐ 9 **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.

☐ 10 **Required:** Define access policies (or edit those loaded in step 7). 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.

☐ 11 **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.

☐ 12 **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 Monitor, Approved, or Rejected. Typically, the intended choice for a policy of this type is Approved or Rejected.

See “Adding an Access Policy” in the Creating Access Policies chapter.

☐ 13 **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.

☐ 14 **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 conflicts generated by the policy.

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 responsibility 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.

☐ 15 **Optional:** Define conditions to create a more focused conflict analysis and eliminate false positives. You can create three types of condition that affect the generation of conflicts:

- 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.

See “Defining Conditions” in the Creating Access Policies chapter.

☐ 16 **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 3 — 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.

Configuration Planning and Installation

You need to create and set up one or more data sources in the AACG Data Administrator. The data sources 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 *Application Access Controls Governor User Guide* for help in completing setups.

Defining Your Data Sources

Before you begin setting up your data sources, 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 data sources so that when policies are loaded or created, they will be able to run against the appropriate data sources.

Defining Your Roles

Before you begin setting up your roles, consider who will use AACG, 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 data sources, 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). This is the only AACG feature *not* assigned to either default role. To implement User Provisioning, therefore, you must create at least one role that includes 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. As you do so, bear in mind that according to accepted practice, a user who creates policies should not be able to review the conflicts it generates. 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 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 AACG 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 data source 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 data source 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 Query Only: **Yes**

  Do not apply access policies to responsibilities that have been registered as query-only, because users cannot transact in such responsibilities.

- 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**

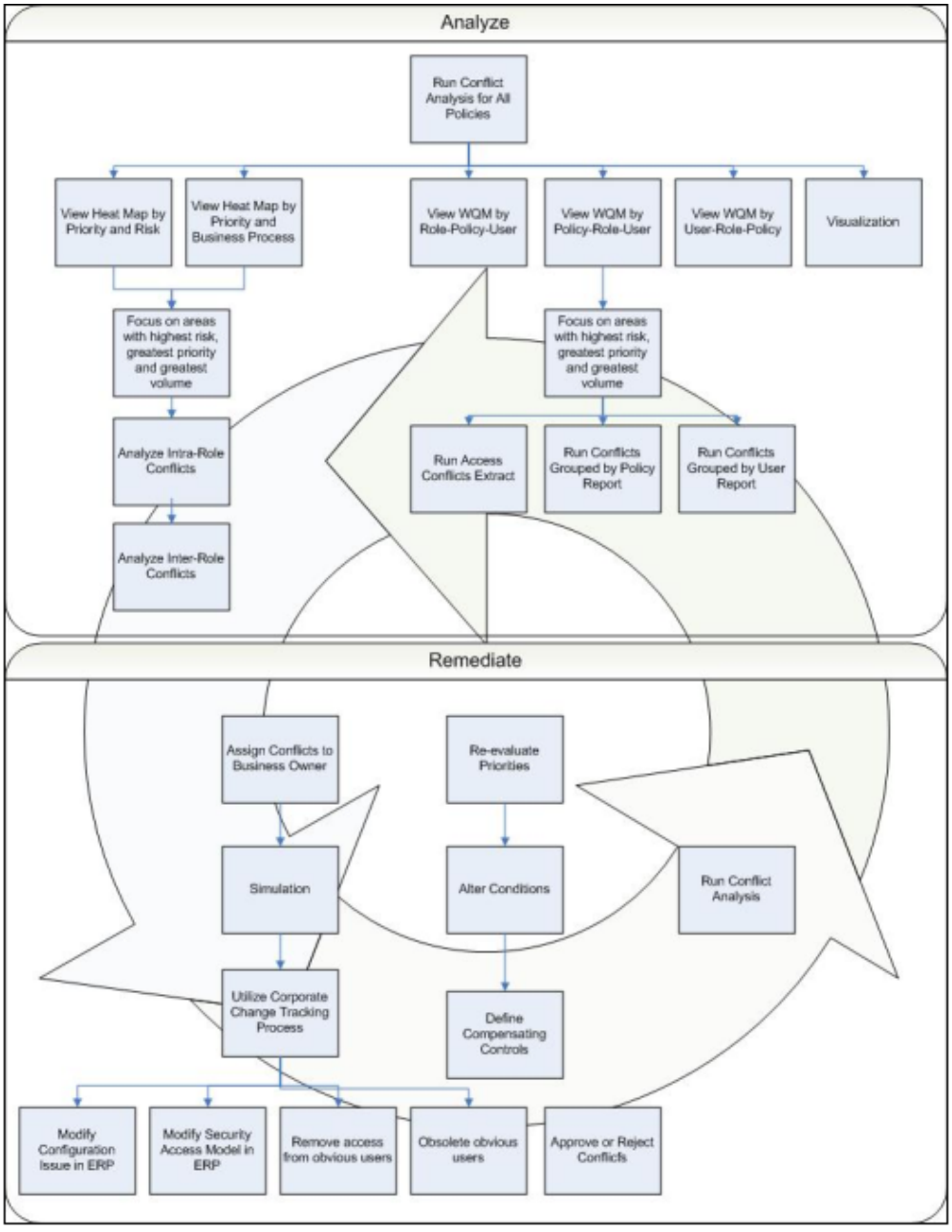
  Responsibility assignments that have been end dated should not be considered in conflict analysis since the user does not actually have access to those responsibilities.

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. 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.

- ☐ 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).

☐ 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.

☐ 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 or add an access point to see how your action would impact your conflicts and your 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 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 or add an access point to see how your action would impact your conflicts 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. A few reports are commonly used to help analyze conflicts:

- Access Conflicts Grouped by User Report

  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 policy. Then run this report for that policy. By doing so, you will get a summary of users that have violated that policy, and be able to quickly see where your biggest issues are.

  You can jump to that user and view all the conflict paths, grouped by that user, policy, and role. If you find access points that conflict with each other in the *same* role, this is an obvious area that needs to be cleaned up. A role should not cause conflicts within itself.

  If you find access points for that policy and user that conflict *across* roles, you have an inter-role conflict that can be cleaned up.

  Through a review of the paths, the access points that conflict with one another should become apparent. Because the full path is given, decisions on how to remediate are made easier. For instance, it may be apparent that removing a function from a menu will resolve several conflicts.

- Access Conflicts Grouped by Policy Report

  A common way to use this report is to resolve 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 by role and then by user of all the paths that conflict.

  Through a review of the paths, the access points that conflict with one another should become apparent. If conflicting access points are seen in different roles for that policy, one of the roles needs to be cleaned up. Because the full path is given, decisions on how to remediate are made easier. For instance, it may be apparent that all of the access points causing the issue are found in one menu, and by removing that menu from that role you would resolve the conflicts.

- 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.

See the Reporting chapter of the *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 write simulation "scenarios." Each scenario comprises a set of rules that instruct AACG to determine how conflict generation would change if configuration of the business-management application were altered. Each rule names an access point that might be excluded from or inserted in another access point — in Oracle EBS, for example, a function that might be excluded from a responsibility, or added to a menu.

Once a scenario is created and run, you can view its results: a display of conflicts that would be resolved or added, or a display of users who would be affected, if the simulated changes were actually implemented in the business-management application. The latter includes users involved in conflicts as well as those with legitimate rights to access points involved in conflicts (since they would be affected if excluding an access point from a responsibility or menu prevented them from accessing it.)

If access policies have changed since the last time the Find Conflicts program was run, you must run it again as part of the simulation process. If access policies have not changed, you can choose whether to run Find Conflicts again, or to use the most recent run:

- Choose to run Find Conflicts if changes have been made in the business management application to components that might be involved in conflicts or in simulation runs — for example, if users have been created or deleted, if responsibility assignments for existing Oracle users or page-definition assignments for existing PeopleSoft users have changed, or the like. Such changes have the potential to resolve existing conflicts in your system or create new conflicts, thus rendering the most recent run of the Find Conflicts program obsolete.
- Choose not to run the Find Conflicts program if such changes have not been made since Find Conflicts was last run in AACG. In that case there is no disparity between the conflicts recognized by AACG and the actual state of your conflicts, and the simulation process runs more rapidly because a new set of actual conflicts need not be generated.

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

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.

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 *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 AACG 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 Oracle Embedded Agent, click on the Form Rules link.
4. A GRC Controls — Oracle Rules form appears. It provides access to three "Embedded Agent" 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:

1 Log on to the PeopleSoft server.

2 During installation of an AACG "Provisioning Embedded Agent," a staging directory was created on the PeopleSoft server. (See the *Installation and Upgrade Guide*.) Navigate to that staging directory.

3 Using a text editor, open a file called peafin.properties. Set its pea.aacg.ps.enabled property to the value *0*. Save and close the peafin.properties file.

4 From the staging directory, execute the following command:

```
jar uf ag-pea-ps-8.2.1-SNAPSHOT.jar peafin.properties
```

5 Stop the PeopleSoft application server

To do so, use the psadmin utility: To start it, execute the command *PS_HOME*\appserv\psadmin (on a Linux server) or *PS_HOME*\appserv\psadmin.exe (on a Windows server). In either case, replace *PS_HOME* with the full path to the highest-level directory in which PeopleSoft components are installed. If necessary, see PeopleSoft documentation for information on using the psadmin utility.

6 Copy the following file from your staging directory to the *PS_HOME*\appserv\classes directory:

```
ag-pea-ps-8.2.1-SNAPSHOT.jar
```

7 Use the psadmin utility to restart the PeopleSoft application server. (See step 5 for information on running the psadmin utility.)

To turn User Provisioning back on, repeat this process, but set the pea.aacg.ps.enabled property to the value *1* in step 3.