Oracle® Governance, Risk and Compliance Controls

Release Notes

Release 8.5

Part No. E25645-01

October 2009

Oracle Governance, Risk and Compliance Controls Release Notes

Part No. E25645-01

Primary Author: David Christie

Contents

1 Release Notes

Transaction Controls Governor.. 1-1

Application Access Controls Governor 1-2

Reports 1-2

Simulation 1-2

Performance Enhancements... 1-3

Conflict Run Purges 1-3

Condition Comments 1-4

Common Functionality... 1-4

Home Page 1-4

Roles and Users 1-4

Data Synchronization... 1-5

Import and Export 1-5

GRCC and Language 1-6

Installation 1-6

Release Notes

Version 8.5 of Oracle Governance, Risk and Compliance Controls (GRCC) provides a platform in which two applications run — Transaction Controls Governor (TCG) and Application Access Controls Governor (AACG). In earlier versions (8.0 through 8.2.1), the platform contained only AACG, and the product was known as Application Access Controls Governor. Version 8.5 adds TCG to the platform, and as a result the product as a whole is renamed Governance, Risk and Compliance Controls.

The applications can impose controls by default on instances of Oracle E-Business Suite and PeopleSoft Enterprise, and may be configured to work with other business-management applications as well.

Transaction Controls Governor

Transaction Controls Governor enables users to define “models,” each of which specifies circumstances under which individual transactions would pose unacceptable risk to a company.

A model consists of one or more “filters,” each of which is a logical statement that defines what makes a transaction risky (or defines one element of that risk, if the model contains more than one filter). A simple filter may state, for example, that the value of an expense report is greater than the amount allowed by company policy.

Each filter specifies a “business object” (a business-language label for one or more database tables that hold information pertinent to a transaction), as well as an “attribute” of that object (a business-language name for a column within the tables). In the example, the expense-report value is the attribute, and belongs to an Expense Report business object.

There are two filter types. A “defined” filter (the type used in the example) enables the user creating the filter to specify its logic. A defined filter may also arrange records of transactions into sets, based on commonality in the values of an attribute. A “pattern” filter employs a statistical function, provided by Oracle, that identifies baselines and outliers to the baseline values.

When evaluated, a model returns records of transactions that exceed the defined risk. TCG retains these records only until the model is run again, when it replaces the earlier results with a new set. The results of each model run may, however, be exported to a spreadsheet and saved there. Models may be created not only by users who intend to investigate suspect transactions, but also by users, such as auditors, who want to assess the risk inherent in a system at a given moment.

For complete information on using Transaction Controls Governor, see the *Transaction Controls Governor User Guide*.

Application Access Controls Governor

Application Access Controls Governor regulates access to duties assigned in business-management applications. It implements “access policies,” which identify conflicting “access points” to business-management applications. Access points are considered to conflict with one another because, in combination, they would enable individual users to complete transactions that may expose a company to risk. New features for version 8.5 include the following.

Reports

Version 8.5 of GRCC uses Oracle Business Intelligence Publisher (BIP) as its reporting engine. Some AACG reports are “seeded” with the application — they can be run either from its Report Center or from AACG pages to which the reports are relevant. (For example, an Access Policy Detail Report, which provides information about configured access policies, may be run from the Report Center or from the page in which access policies are defined.) These require no setup beyond the installation of GRCC itself.

However, other reports are offered as “BIP Templates.” These enable users to employ BIP functionality to modify report layouts. Templates are “decoupled” from GRCC, which means that report templates are downloaded from My Oracle Support (Metalink), and may be offered between GRCC releases.

The BIP Templates must run on a server separate from the GRCC server. To run them, one would create a distinct “Data Analytics” schema on the BIP server, install an instance of Business Intelligence Publisher, create a JDBC connection from BIP to the Data Analytics schema, and use a GRCC Analytics Configuration page to connect GRCC to the Data Analytics schema.

For information on the seeded reports, see the *Application Access Controls Governor User Guide*. For descriptions of individual report templates, see readme documentation that accompanies template releases. For information on setting up an instance in which to use the BIP Templates, see the BIP for GRCC Admin/Implementation Guide and the Governance, Risk and Compliance Controls User Guide.

Simulation

An AACG simulation feature enables users to forecast the effects of “cleanup” — actions taken in business-management applications to resolve conflicts that AACG has uncovered. In version 8.5, simulation is significantly redesigned and enhanced.

Typically, cleanup involves identifying an access point involved in a conflict, then “removing” it from a “parent” access point through which users can reach it. In an

Oracle EBS context, for example, one might remove a function from a menu, or a menu from a responsibility.

Simulation in version 8.5 offers the ability to configure such removals graphically. Users can create “models” — each a diagram of the connections between a selected access point and all others that relate to it as parents or children (through all generations). Within the model, the user can easily select one or more parent-child pairs; color coding in the model then shows how removal of the child from the parent would cut off access throughout the complex of access points.

Each removal creates a step in a “remediation plan.” When the user has created all the steps he wants, he can run the remediation plan and see results — counts of the conflicts (or conflict paths) that would be eliminated or created if the removals were actually implemented in the business-management system, in total and by user, policy, role and other measures.

Simulation “scenarios” created in earlier 8.*x* versions of AACG are incompatible with version 8.5. If you wish to reuse simulation plans you created in earlier versions, you need to re-create them in version 8.5. For information on simulation, see the *Application Access Controls Governor User Guide*.

Performance Enhancements

AACG pages may display lists. For example a Definition page, in which users create access policies, contains a list of configured policies. The Conflict Analysis page and the Work Queue, in which users review conflicts, contain lists of conflict paths. In such lists, users can create “views.” These filter the contents of a list and otherwise configure its display.

In earlier versions, a Clear View button would restore the full display of every possible item in a list. Because lists (particularly of conflict paths) could be quite large, this could impact performance. In version 8.5, clicking on the Clear View button causes all entries to disappear from the list. To restore content, the user has the option of selecting (or defining) another view, or of clicking on a View button to display all possible entries.

In the Definition page (in which access policies are created or edited), the Entitlements page (where access points may be gathered into sets for use in access policies), and the Work Queue (were status is assigned to conflicts), version 8.5 enables users to modify more than one item, and then save all modified items in one save operation.

In the Definition page, users can employ a “mass edit” feature to reset the status or type of multiple policies at once. In the Work Queue, users can set the status of multiple conflict paths at once. In earlier versions, however, a user could select items to update only from those that were visible on screen at any one time — typically a small subset of all possible items. In version 8.5, however, the user can create a view, then perform a mass edit on all items in the view, even if some are not actually displayed on screen.

Conflict Run Purges

AACG users may run a Find Conflicts program, which evaluates business-management-application users, noting those whose work assignments violate access policies. Each run of the Find Conflicts program generates a distinct set of results, and AACG pages may display results of individual runs, or a cumulative set of results. Version 8.5 introduces the ability to purge individual runs of the Find Conflicts program. For more information, see the *Governance, Risk and Compliance Controls User Guide*.

Condition Comments

Users can create policy-based, path-based, or global conditions, which specify exemptions to policies or otherwise specify circumstances under which the policies are enforced. Version 8.5 provides fields in which users can comment upon the conditions they create.

Common Functionality

Although TCG and AACG have distinct feature sets, they also share some functionality provided by the GRCC platform. These features include tools to connect GRCC to Oracle, PeopleSoft, and other business-management-application data sources (instances), and to refresh “snapshots” of data gathered from those applications; to create GRCC users and user roles; and to set GRCC parameters, connect with your email server (for the purpose of sending notifications to GRCC users), and integrate GRCC with other applications. Moreover, the GRCC platform can display information in any of eleven languages.

Version 8.5 introduces a new home page and changes several of the existing common features.

Home Page

In version 8.5, the GRCC home page contains two graphs. A bar graph depicts the ten TCG models that have identified the greatest numbers of risky transactions; each bar represents a model, its height proportional to the number of transactions identified by that model. A pie graph depicts the ten AACG access policies that have generated the greatest numbers of conflicts; each “pie slice” represents a policy, its area proportional to the number of conflicts generated by that policy. When a user clicks on a bar in the TCG graph or a pie slice in the AACG graph, a grid below the graphs displays information about the transactions or conflicts returned by the selected model or policy.

Roles and Users

In GRCC, administrators define roles — each a selection of TCG, AACG, and common features available to users — and then assign roles to users. Each user has access to the functionality offered by his roles.

In earlier versions, an administrator would define a role by selecting pages to which a user could navigate, with either view or update permissions. In version 8.5, the administrator not only specifies GRCC page access, but also selects data sources and business objects that role members can use to create TCG models. (Page-access selections apply to TCG, AACG, and common features. Data source and business object selections, however, are specific to TCG.)

Moreover, in version 8.5 one can define “user roles” and “group roles.” A user role is a selection of privileges available to members of the role. A group role is a set of two or more roles that confers all access defined by the constituent roles, any of which may itself be a user or group role.

In earlier versions, a default “admin” role provided access to all pages except the AACG User Provisioning Requests page. (In that page, GRCC users may review access-policy violations that AACG discovers as privileges are being assigned to business-management-application users.) In version 8.5, however, the admin role has access to all GRCC pages and features, including User Provisioning Requests.

As in earlier versions, one creates roles, then creates user accounts and assigns roles to them. In version 8.5, however, User Administration features are enhanced. For example, the User Administration page in earlier versions enabled administrators to specify general information about each user and to assign roles. The version 8.5 User Administration page does the same, but also enables administrators to view the privileges offered by each of the roles.

For complete information on role and user administration, see the *Governance, Risk and Compliance Controls User Guide*.

Data Synchronization

AACG access policies and TCG models work with snapshots of data from external data sources — the business-management applications in which GRCC implements controls. GRCC users must periodically “synchronize” data — update the snapshots to capture changes made in a data source since the last time data was synchronized. Typically, one would perform data synchronization before evaluating AACG access policies or before running TCG models, to ensure that business-management-application data is as current as it can be.

Version 8.5 adds the ability to synchronize data used by TCG. As before, data synchronization may either be scheduled or be run ad hoc. In version 8.5, however, data synchronization operations update information used by AACG or by TCG, but not both. As before, a user runs (or schedules) data synchronization from a Synchronize option on a Data Administration page (in which users also configure connections from GRCC to data sources). In version 8.5, this option enables the user to select whether to synchronize data used by AACG or by TCG.

From the AACG Definition page (in which access policies are created), users may run the Find Conflicts program against specific policies, and may schedule it to be run. While creating schedules, they may choose to synchronize data before each scheduled Find Conflicts run, and this synchronization operation is specific to AACG.

Similarly, TCG users may run synchronization from a Manage Models page, and this synchronization operation is specific to TCG.

Import and Export

GRCC users may export AACG access policies or TCG models from a GRCC instance to files, and may import them from files to GRCC instances. In TCG in particular, the Manage Models page displays only the models created or imported by the user who is currently logged on; thus import and export are the means by which users may share models with one another. (Also in TCG, models may be imported and exported as actual models, or as templates for the creation of new models.)

Within each application, an export operation works similarly to the way it worked in past versions of AACG. A user selects objects to export (models in the TCG Manage Models page or policies in the AACG Definition page), selects an export menu option, and designates a location in which the export file should be saved.

Import functionality, however, is changed in version 8.5. A user may select a file containing objects to be imported — models in TCG or policies in AACG. The user may then select individual objects from the file, and thus import only those objects. Finally the user designates data sources in the target instance that should be associated with imported objects.

Version 8.5 also offers enhanced error logging during import and export. In AACG, for example, logs provide links to view errors within the application, which give exactly the policy, entitlement, and any failed access point names and IDs.

For information on exporting and importing access policies, see the *Application Access Controls Governor User Guide*; for information on exporting and importing models, see the *Transaction Controls Governor User Guide*.

GRCC and Language

Version 8.2 of AACG introduced the capability to display information in multiple languages. Version 8.5 extends this capability to TCG. In version 8.5, supported languages include US English, standard and traditional Chinese, Danish, French, German, Italian, Japanese, Korean, Brazilian Portuguese, and Spanish. French Canadian is no longer supported.

Installation

As you install GRCC, you may install “provisioning embedded agents” (PEAs) in instances of Oracle E-Business Suite and PeopleSoft Enterprise in which GRCC is to implement controls. These PEAs support the User Provisioning feature of AACG. For each PEA you install, you must designate a GRCC user and password. However, GRCC passwords expire every 90 days, and so the passwords for the PEA users must be reset every 90 days. The installation package for version 8.5 of GRCC includes a utility that resets passwords for PEA users. For information on its use, see the *Governance, Risk and Compliance Controls Installation and Upgrade Guide*.