Oracle® Governance, Risk and Compliance Controls

Release Notes

Release 8.6.0

Part No. E25619-01

September 2010

ORACLE

Oracle Governance, Risk and Compliance Controls Release Notes

Part No. E25619-01

Primary Author: David Christie

Contents

Release Notes

Release Notes

Oracle Governance, Risk and Compliance Controls (GRCC) provides a platform in which two components run: Application Access Controls Governor (AACG) regulates access to duties assigned in business-management applications such as Oracle E-Business Suite and PeopleSoft. Enterprise Transaction Controls Governor (ETCG) identifies business-application transactions that pose unacceptable risk.

Access and Transaction Analysis

In version 8.5.1, TCG users could create "models," which defined transaction risk and returned "temporary" results — snapshots of risk that were replaced each time models were run. In version 8.6.0, ETCG users can not only create models, but also convert them into "controls," which return "permanent" results — records of violations that remain available to be resolved no matter how often controls are run.

In version 8.5.1, AACG users could create "access policies," which defined conflicts among "access points" in a business application and identified users with conflicting access. In version 8.6.0, AACG adopts a structure like that of ETCG: Users can create access models, which return temporary results, and can convert them into access controls, which return permanent results. Both access models and controls continue to specify access points that, in combination, would enable individual users to complete transactions that may expose a company to risk.

In version 8.5.1, a TCG model comprised elements — filter, function, or pattern — each of which defined some aspect of risk and returned records of transactions that satisfied the definition. In a graphic interface, any number of these elements could be arranged in a pattern that defined a processing logic — AND or OR relationships that determined the results a model would produce. Each of these elements specified an "attribute" of a "business object," which roughly corresponded to a column in a database table that supplied data for analysis. In version 8.6.0, an ETCG control inherits the filtering elements and processing logic from the model that is its source.

In version 8.6.0, AACG models and controls are developed similarly. An AACG model uses filters arranged graphically in an AND/OR pattern. Its filters may specify access points (or "entitlements" — selections of access points); their AND/OR relationships define risky combinations. Or filters may define "conditions" — exemptions from processing. Each AACG filter also specifies an attribute of a business object,

which can supply an access point, an entitlement, or a value used in a condition. Each AACG control inherits the filters and processing logic from its source model.

As a model is converted into a control, a user adds items necessary for "incidents" (control violations) to be resolved. For example, each control requires at least one "participant" — a person (or group) assigned to resolve incidents. Users may also apply "tags," or values by which controls and their incidents can be categorized. (These were known as "dimensions" in earlier versions.) In version 8.6.0, participants and tags apply to both AACG and ETCG analysis.

AACG can discover conflicts that existed before controls were written to protect against them ("detective" analysis), or intervene when a user is assigned duties after controls have been written to define them as conflicting ("preventive" analysis). ETCG implements only detective analysis, uncovering suspect transactions that have been completed before a control is run.

In version 8.6.0, there is no change to preventive analysis by access controls. However, the assignment of status to incidents discovered through detective processing is unified for AACG and ETCG. Version-8.5.1 conflict-resolution tools such as the Conflict Analysis page, the Work Queue, and the Heat Map no longer exist.

The GRCC platform provides pages, shared by AACG and ETCG, for the management of models and controls, and for the resolution of incidents.

Each of the control- and incident-management pages enables users to edit values for multiple controls or incidents at once. For both controls and incidents, these values include comments, participants, and status. For controls, values also include priority and tags.

From the home control- and incident-management pages, users may also open pages that display full details for individual controls or incidents.

Version-8.6.0 changes to AACG-specific features include the following:

- A simulation feature enables AACG users to forecast the impact of incident resolution on business-management applications. In version 8.6.0, users can select one or more controls, and base simulations on the resolution of their incidents.
- A visualization feature enables users to depict graphically the paths from any number of users to any number of access points involved in conflicts. In version 8.6.0, this feature is available from windows in which users view model results.
- In earlier versions, AACG tracked individual runs of the program it used to analyze access policies, displaying either a "cumulative" view of conflicts or the conflicts generated in any run of the analysis program. In version 8.6.0, AACG maintains one consolidated record of incidents generated by all runs of control analysis.

Version-8.6.0 changes to ETCG-specific features include the following:

- The Business Object Library for ETCG includes SOD objects for use in transaction analysis.
- ETCG enables users to import any set of data as a "custom object" and use it as if it were a business object. In version 8.6.0, custom objects can be deleted.

Reporting

GRCC 8.6.0 expands the reporting capability to include not only reports on AACG analysis, but also ETCG analysis, as well as GRCC users and roles. Reports include the following:

- Control Detail Extract Report provides information about both access and transaction controls.
- Conditions Report provides information about control-specific, global, and global path conditions that may be set in AACG.
- Global Users Report provides information about IDs created by GRCC, each of which correlates to any number of potentially varying IDs a person may have in business-management applications subject to access controls.
- Incident Summary Extract Report lists incidents generated by access and transaction controls.
- Incident by Control Summary Extract Report lists access and transaction controls that have generated pending incidents.
- Transaction Incident Details Extract Report provides details of incidents generated by transaction controls.
- Access Incident Details Extract Report provides details of incidents generated by access controls.
- Access Point Report lists paths to access points involved in conflicts.
- Access Violations by User Report lists the ten users with the greatest number of conflicts, as well as the number of conflicts for each.
- Access Violations Within a Single Role Report lists roles for which access controls generate "intra-role" conflicts.
- Intra-Role Violations by Control Report lists access controls that generate intra-role conflicts.
- Users with Access Violations by Control Report lists access controls that have generated conflicts.
- GRCC Users and Roles Report provides information about GRCC users and the GRCC roles assigned to them.

Administration

The GRCC platform provides tools to connect to Oracle EBS, PeopleSoft, and other applications and to "synchronize" its data with that of business applications; to create GRCC users and roles; to set GRCC parameters, connect with your email server, and integrate GRCC with other applications.

In version 8.6.0, the GRCC properties an administrator can set include the number of login attempts a user may make before being locked out of the application, and the number of days before a password expires. Administrators may also set an "Enable analysis across datasources" switch to optimize performance if each control is configured to apply only to a single datasource.

Moreover, the pages on which administrators can complete administrative tasks — such as importing business objects or patterns —have been reorganized.

GRCC displays information in multiple languages, and Dutch has been added. (Administrators use a Properties page to select the languages they want to make available to users.) The languages available in version 8.6.0 total twelve: US English, traditional Chinese, standard (simplified) Chinese, Danish, Dutch, French, German, Italian, Japanese, Korean, Brazilian Portuguese, and Spanish.

Installation

You can perform a "fresh" installation of GRCC 8.6.0, or you can upgrade to it from version 8.5.1. You cannot upgrade directly to it from any earlier version; instead, you must upgrade an earlier version to 8.5.1, and then upgrade from there to 8.6.0. See the *Oracle Governance, Risk and Compliance Controls Installation and Upgrade Guide* for details.

Resolved Issues

Version 8.6.0 incorporates corrections to issues identified during the use of version 8.5.1. These include the following:

- Issue 8719024: User can filter controls by tag value and run only the tagged controls.
- Issue 8972589: In LOVs, user can begin to type a value to generate a list filtered by the value typed.
- Issue 8992821: For a pattern used in a transaction model, label text was saved, but not displayed when the pattern was reloaded.
- Issue 9003208: In model results, a datasource ID value is replaced by the name of the datasource corresponding to the ID.
- Issue 9007747: In the Manage Models page, a grid that displays entries for models offers column sorting.
- Issue 9021131: When a Delete action is performed from the My Models action drop-down, removing the model should also remove/purge the corresponding data results tied to the model.
- Issue 9025154: For a transaction model that uses a pattern, values are sorted alphanumerically on the x-axis.
- Issue 9259582: Exclusions to access analysis defined by global conditions were not recognized in reports.
- Issue 9291080: The Manage Jobs page generated an unexpected error during an attempt to purge jobs.
- Issue 9305875: Attempts to generate reports resulted in errors.
- Issue 9385371: Attempts to use the AACG Visualization feature resulted in errors.

- Issue 9439868: When ETCG synchronization was run from the Manage Application Data page, the status of the run was not updated correctly in the Jobs and Scheduling page.
- Issue 9468689: Business objects assigned to a GRCC role were not being saved.
- Issue 9497913: An attempt to run access simulation statistics resulted in an error.
- Issue 9541854: Concurrent requests used for preventive analysis in Oracle EBS instances generated errors.
- Issue 9553230: An attempt to edit control status generated errors.
- Issue 9567515: A table supporting custom adapters was not being populated. (Custom adapters — called custom connecters in version 8.6.0 — enable GRCC to apply models and controls to applications other than Oracle EBS and PeopleSoft.)
- Issue 9578470: Imports of pre-built policies (called controls in version 8.6.0) failed.
- Issue 9740629: AACG conflict analysis generated an "ODM Issue Clarification" error.
- Issue 9792943: AACG conflict analysis failed when run against a "view" (a filtered set of policies/controls).
- Issue 9846065: Conditions were written to exclude Oracle EBS functions from access analysis, but they were included anyway.
- Issue 9816911: A global condition to exclude "no prompt" functions from access analysis failed.
- Issue 10105065: When AACG preventive analysis presented a role assignment for review in the Manage Access Approvals page, an attempt to reject the assignment produced an error.
- Issues 10105077 and 10105579: The review of role assignments identified as violations of access controls by AACG preventive analysis, and the approval of those roles, took excessive time.