Oracle® Governance, Risk and Compliance
Release Notes
Release 8.6.4.3000
Part No. E36201-01

August 2012

ORACLE®

Oracle Enterprise Governance, Risk and Compliance Controls Release Notes

Part No. E36201-01

Contents

Release Notes

Release Notes

Oracle Governance, Risk and Compliance (GRC) is a set of components that regulate activity in business-management applications:

- Oracle Enterprise Governance, Risk and Compliance Controls (EGRCC) comprises two elements, Application Access Controls Governor (AACG) and Enterprise Transaction Controls Governor (ETCG). These enable users to create models and controls and to run them within business applications to uncover and resolve segregation of duties violations and transaction risk.

- Oracle Enterprise Governance, Risk and Compliance Manager (EGRCM) forms a documentary record of a company's strategy for addressing risk and complying with regulatory requirements. In enables users to define risks to the company's business, controls to mitigate those risks, and other objects, such as business processes in which risks and controls apply.

- Fusion GRC Intelligence (GRCI) provides dashboards and reports that present summary and detailed views of data generated in EGRCM and EGRCC.

In GRC 8.6.4.3000, these GRC components run as modules in a shared platform. EGRCC runs as a Continuous Control Monitoring (CCM) module. EGRCM provides a Financial Governance module by default, and users may create other EGRCM modules to address other areas of the company's business. A customer may license only EGRCM, only AACG, or only ETCG; any combination of them; or all of them.

Because these components share a common platform, they also share some functionality. In general, where earlier versions of EGRCC and EGRCM had similar features, the GRC 8.6.4.3000 platform adopts the EGRCM standard.

The following are prominent among the changes for version 8.6.4.3000:

EGRCC used "tags," and EGRCM used "perspectives." Each was, in effect, a set of related values; users could classify objects (such as risks, models, or controls) by associating individual tag or perspective values with them. However, perspectives are more powerful: First, they are hierarchical, with individual values having parent/child relationships to other values. Second, they play an important role in security: "data roles" may be associated with perspective values, and so grant access only to data objects that are associated with the same perspective values. Version 8.6.4.3000 embraces the use of perspectives, and discontinues the use of tags.

(When a customer upgrades from version 8.6.3 of EGRCC, tags are converted to perspectives automatically.)

GRC 8.6.4.3000 also adopts the EGRCM security system. In this system, "duty roles" define narrowly focused sets of privileges and are combined into broader "job duty roles." "Primary data roles" specify narrowly focused sets of data and are combined to form broader "composite data roles." Finally, "job roles" combine job duty roles with composite data roles, and are assigned to users. GRC 8.6.4.3000 discards the security system that existed in earlier versions of EGRCC (although, once again, during an upgrade from version 8.6.3 of EGRCC, roles are constructed automatically so that users have the same access in the later version as they had in the earlier).

Version 8.6.4.3000 issues "worklists" (each a record of a task that requires its recipient to act) and "notifications" (each a record of a task in which a recipient has an interest, but need take no action). In earlier versions, EGRCM incorporated worklists and notifications, but EGRCC did not.

Revised search and saved-search functionality replaces the "views" that existed in earlier versions of EGRCC.

Some administrative features are reorganized. For example, features that had been available from tabs on a single administration page in earlier EGRCC versions are now divided among Manage Application Datasources and Manage Application Libraries pages.

GRC may be configured to support Secure Sockets Layer (SSL), although this is optional. While EGRCM previously had to be installed with WebLogic Server, GRC 8.6.4.3000 may use either WebLogic or Tomcat Application Server (as was true for EGRCC in past versions).

Issues Resolved in EGRCM

Version 8.6.4.3000 resolves the following issues in Enterprise Governance, Risk and Compliance Manager:

- Issue 14307241: Display of related components in the perspective viewer showed incorrect object types as well as incorrect objects dependent on the type of object selected, and did not show child components of displayed components.

- Issue 14291980: In each of the pages in which users create or edit objects, they can attach documents. However, attached documents were blank when users attempted to retrieve them.

- Issue 14263061: Data Migration — the import of operational data to an EGRCM instance — generated an error. After import, the system became unstable, data was inconsistent, and performance was poor.

- Issue 14245483: An attempt to run the Issue Details Report generated an error.

- Issue 14216369: EGRCM stores selections available in certain lists of values as "lookups," which are user-configurable. (These include, for example, perspective types, assessment types, or survey types.) The application did now show a proper message when lookup values exceeded character limits.

- Issue 14181591: For each "lookup type" (which distinguishes lookups belonging to one LOV from those belonging to others), each entry correlates a "lookup code" to a "meaning," the latter being the text that actually appears in an LOV. The Control Assessment Extract Report should have displayed lookup meanings, but displayed codes instead.

- Issue 14104305: When GRC incorporates GRCI, GRC makes use of a "data analytics" (DA) schema, which is distinct from the principal GRC database schema. When the DA schema was updated, data was written to it in ABC order.

- Issue 14103436: The Risk Control Matrix report, which should list EGRCM risks, controls, or processes and related information, did not run.

- Issue 14098317: When a related risk was added to a process, the add pop-up did not display the description configured for the risk. The description was therefore also omitted from the create, edit, and manage process pages.

- Issue 14082656: Users may assess objects and perspectives periodically, to determine that they are defined and implemented correctly when created, or that their definition and implementation remain appropriate as time passes. If initiated through Assessment Management, an assessment is based on a plan, which in turn is developed from a template. Users were unable to edit a saved plan and select a blank template.

- Issue 14065220: A Report History section of the Report Management page displays a row for each generation of a report that has been scheduled to run. Users should be able to select a row and view the generated report, but attempts to view the Control Details Report resulted in an error.

- Issue 14050982: Status of a Data Analytics update (and other jobs) is reported in a Manage Jobs page. Although this page showed a Data Analytics update as completed, details available from a Message field showed the job as being only 10 percent complete.

- Issue 14049059: A new lookup for the GRC_SURVEY_QUESTION_TYPE lookup type generated an error.

- Issue 14044429: Any report that included a user-defined attribute (UDA) field showed the value of that field as a lookup code rather than a lookup meaning.

- Issue 14009376: Each perspective hierarchy becomes available for use with objects only after being associated with that type of object in the Manage Module Perspectives page. In the process, a perspective may be designated as required (at least one perspective value must be selected for each object of the associated type). In past version this designation could not be edited once data existed in the module. In 8.6.4.3000, a required perspective can be changed to optional, but an optional perspective cannot be changed to required.

- Issue 13986970: When controls are related to a risk, they may be assigned "stratification" values that depict how they work together to mitigate the risk. The available values are lookups stored in a lookup table. Users could not edit these values in that table.

- Issue 13981650: When notifications were enabled in the Manage Application Configurations page, uses who completed design review assessments received

multiple notifications, the content of which was not in sync with the status of the assessment.

- Issue 13947709: In a Manage Configuration Options page, a user can choose the features available for each object within an EGRCM module, and define how assessments are conducted for the object. For example, the user can edit "guidance text," a statement of purpose that users may consult while completing an assessment activity. However, edits to this page could not be saved.

- Issue 13942124: When users scheduled reports to be run, the reports did not appear in the queue after the schedule time.

- Issue 13921920: Comments for all objects should be included in the DA schema.

- Issue 13915592: In the Control Assessment Report, invalid users were displayed for assessors, reviewers, and approvers.

- Issue 13915370: In the Control Assessment Extract Report, invalid users were displayed for assessors, reviewers, and approvers.

- Issue 13890328: GRC can be integrated with an OID LDAP server that manages GRC users. However, an "Import from LDAP" job returned no data, although a large number of users existed in the OID directory.

- Issue 13857808: Users attempted to initiate assessments that did not complete.

- Issue 13852279: Complete assessment not returning results.

- Issue 13811933: The Edit button is active on the Control Overview page for a user who does not have edit access to controls.

- Issue 13800232: During an assessment, users were unable to see risks related to a control in the related-object section.

- Issue 13789548: Users may create test plans for controls, each consisting of set of instructions users follow to verify that the control serves its purpose in mitigating risk. However, test plans could not be created for controls in custom modules.

- Issue 13775177: The Edit button is active on the Process Overview page for a user who does not have edit access to processes.

- Issue 13770990: Edits to perspective values disrupted a security system in which data roles were associated with values from that perspective.

- Issue 13743908: When a user viewed related components for a perspective item via the perspective viewer in Manage Risk, all objects were not returned.

- Issue 13743625: When notifications were enabled in the Manage Application Configurations page, users received email messages concerning both worklists (which required action) and notifications (which did not require action). Beginning with version 8.6.4.3000, users will receive email messages concerning worklists only.

- Issue 13723462: Users may schedule reports to be run, in which case a record of each schedule appears in a Manage Scheduling page. From that page, a user should be able to click a Run Now button to run the report manually, but this option did not work.

- Issue 13646196: When a new module was created, assessment objects (such as a template) were created in it, and the name of the custom module was subsequently changed, the assessment objects were lost, and an error was displayed.

- Issue 13633192: When a user created an issue for a control assessment, the Assessment Activity Detail Report showed an invalid Activity field for that control assessment.

- Issue 13097854: Seeded roles were created so that a user could not be granted access to Manage Users and Manage Roles pages without also being granted access to Application Administration.

- Issue 13077108: Attempts to run the Issue Details Report and Issue Listing Extract Report generated errors.

- Issue 13061563: Users were unable to edit a module after creating an instance of an object included in the module.

- Issue 12667864: A Pending Activity report displays outstanding worklist items by user. In the report, a User column showed the user who created the worklist, rather than the user to whom it was assigned.

Issues Resolved in EGRCC

Version 8.6.4.3000 resolves the following issues in Enterprise Governance, Risk and Compliance Controls:

- Issue 14345337: AACG preventive analysis enforces continuous controls as roles are assigned to users in business applications. Depending on the control's "enforcement type," access to a role is either permitted, prevented, or suspended pending approval. In Oracle EBS, when a role was assigned to a user, preventive processing generated an error.

- Issue 14337678: A "datasource" is an instance of a business application subject to EGRCC models and controls. Users configure datasources, and "synchronize" data (update GRC with changes made in the datasources). When a transaction control was created and associated with a datasource, that datasource was subsequently synchronized, and the control was analyzed, the application reported that synchronization was unsuccessful.

- Issue 14050180: "Incident results" are violations of EGRCC continuous controls. A Manage Results page displays records of incidents in a grid, in which users may filter results on column values. Users may also add columns to the grid, but filtering did not work on added columns.

- Issue 13826920: Transaction synchronization worked when run manually, but did not work when scheduled.

- Issue 13770895: Result Management reports ran correctly if a status value was supplied as a parameter, but generated an error if the status parameter field was left blank.

- Issue 13503311: The Users with Access Violations by Control Report lists access controls that have generated incidents at certain statuses; for each control, it lists users whose work assignments have violated the control. However, it listed duplicate records of users.

- Issue 13078891: In the Manage Results page, users may view a list of incidents, or a list of controls that have generated incidents. In the control view, a pending incident count was not updated correctly as incidents were assigned to users.

- Issue 12967875: Some reports can generate results in a format intended for export to Excel. However the Users with Access Violations by Control Report generated multiple files with overlapping data.

Known Issues

The following issues are known to exist in version 8.6.4.3000 of GRC, and will be addressed in future releases:

- Issue 14511156: The import template used by the Data Migration feature includes worksheets for objects other than those configured for a selected module.

- Issue 14472666: A data role intended to define rights to EGRCC data includes a CCM Type value, which determines whether the role grants rights to access or transaction data. A role should allow only one CCM Type value to be selected.

- Issue 14472659: A data role intended to define rights to EGRCC data includes a Business Object value, which determines the business object (set of related data points within a datasource) to which the role grants access. A role should allow only one Business Object value to be selected.

- Issue 14472646: A data role intended to define rights to EGRCC data includes a Datasource value, which determines the datasource (instance of a business application subject to EGRCC controls) to which the role grants access. A role should allow only one Datasource value to be selected.

- Issue 14462303: When a survey template is created (for use with EGRCM), its Delete button is not enabled.

- Issue 14393243: When GRC is configured appropriately, an Intelligence tab displays GRCI dashboards and reports. (This tab may be available from the home page or from object-overview pages.) When a custom module is created, the Intelligence tab is empty.

- Issue 14383638: The Results Management page of the CCM module should display only pending incidents (those at the Assigned and Remediate statuses), but displays incidents at other statuses as well.

- Issue 14349909: If a CCM model is run with a "Within Same Operating Unit" condition, it should detect conflicts only if conflicting access points exist within a given operating unit. Under certain circumstances involving the MO:Security Profile, such a model does not detect conflicts that it should find.

- Issue 14305510: AACG conflict-analysis reports display responsibility names in the Role column, rather than the associated role name from UMX.

- Issue 14297866: AACG is unable to detect user-responsibility assignments when they are made indirectly through UMX.

- Issue 14262826: The import template used by the Data Migration feature includes state for perspective items. This should be removed because perspective items no longer have state.

- Issue 14260552: All issue viewers can view issues on perspective hierarchies, even those without a perspective viewer job role.

- Issue 14247135: In the Manage Roles page, a search for roles produces incorrect results in some circumstances.

- Issue 14230151: Manage UDAs > Module > Assessment option should not exist.

- Issue 14216804: AACG includes a visualization feature — a graphic depiction of paths from any number of users to any number of access points involved in conflicts. If such conflicts are generated by a control that is subsequently upgraded, and control analysis is not rerun, visualization generates an error.

- Issue 14065109: In Survey Management (used by EGRCM), a search on description, status, or state parameters returns no results.

- Issue 13802691: CCM search features include Match All (return only objects that match all search parameters) and Match Any (return objects that match any one or more of search parameters). In the Manage Controls page, Match Any/All should be included only for an "advanced" search.

Installation

To install GRC, you will use a file called grc.ear (if you run GRC with WebLogic) or grc.war (if you run GRC with Tomcat Application Server). You will be directed to validate the file by generating a checksum value, and comparing it with a value published in these *Release Notes*. Your checksum value should match one of the following:

- grc.ear: `faf6a24146f8d830e131e0979d57c6ee`

- grc.war: `0d23bbafb6552e1928b8cebd21519e0c`

For more information, see the *Governance, Risk and Compliance Installation Guide*.