Oracle® Enterprise Governance, Risk and Compliance

Release Notes

Release 8.6.6.4000

Part No. E83507-01

January 2017

Oracle Enterprise Governance, Risk and Compliance Release Notes

Part No. E83507-01

Primary Author: David Christie

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable.

U.S. GOVERNMENT RIGHTS

The software is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications which may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

The software and documentation may provide access to or information on content, products and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third party content, products and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third party content, products or services.

Contents

Release Notes

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

- Oracle Application Access Controls Governor (AACG) and Oracle Enterprise Transaction Controls Governor (ETCG) enable users to create models and "continuous controls." These uncover segregation of duties (SOD) conflicts and transaction risk within business applications. AACG and ETCG belong to a set of applications known collectively as "Oracle Advanced Controls."
- 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. Users can define business processes, risks that impact those processes, and controls that address the risks.
- Fusion GRC Intelligence (GRCI) provides dashboards and reports that present summary and detailed views of data generated in EGRCM, AACG, and ETCG.

These GRC components run as modules in a shared platform. AACG and ETCG run as a Continuous Control Monitoring (CCM) module. EGRCM provides a Financial Governance module by default, and users may create custom 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.

Resolved Issues

Version 8.6.6.4000 resolves the following issues:

- Issue 25239727: The Transaction Incident Details Extract Report lists incidents — records of control violations — generated by ETCG controls. When a value returned in any record included a double colon (::), subsequent values appeared in the wrong columns.
- Issue 24913709: Each CCM control designates result investigators — users authorized to resolve incidents generated by the control. To do so, it uses perspectives, which are sets of related, hierarchically organized values. A control specifies one or more perspective values; result investigators are CCM users whose roles specify the same perspective values. A control may be configured to select one of these users to resolve incidents, or enable any of them to do so.

For a given incident, a result investigator may assign new perspective values and select a new result investigator from the new set of users whose roles contain matching values. If this was done for an AACG incident, and AACG control analysis was subsequently run, the application incorrectly restored the original result investigators.

- Issue 24622460: In AACG, a simulation feature previews how resolutions of access incidents would affect the business application in which those incidents exist. An attempt to delete an unsaved simulation generated an error.
- Issue 24609755: In the Financial Governance module of EGRCM, users may work with Process objects, Risk objects, and Control objects. In the work area for each of these objects, a user selects tabs to work with individual features of the object. Selecting repeatedly among these tabs generated an error.
- Issue 24609677: While editing a perspective hierarchy, users were unable to select Inactive status for nodes of the hierarchy (other than the root node).
- Issue 24609652: GRC can be configured to send e-mail messages to users when tasks require their attention. However, a job to send these notifications generated an error.
- Issue 24569348: Distinct database schemas support GRC and GRCI. The Data Analytics (DA) schema, which supports GRCI, is refreshed by the GRC schema. After an upgrade from version 8.6.6.1000 to 8.6.6.2000, a view within the DA schema, GRI_D_COMMENT_VL, was in an invalid state.
- Issue 24369449: In the EGRCM Manage Risk page, a search returned only 25 records even though more that 25 records contained the string specified as the search parameter.
- Issue 23536568: Users may set status for multiple incidents, or write comments for them, all at once. To select a set of access incidents for mass edit, a user should be able to filter for incidents concerning a global user. In that case, however, the pop-up window to perform the mass edit did not open. (Global users are IDs created for AACG. Each identifies one person, but correlates to any number of potentially varying IDs that person may have in business applications subject to access controls.)
- Issue 23092164: During an upgrade from version 8.6.5.8000 to 8.6.5.9500 to 8.6.6.1000, incidents that had been generated by AACG controls were improperly closed.
- Issue 23048405: When GRC was integrated with Oracle Access Management (OAS) Single Sign On (SSO), attempts to log off of GRC produced no result, and the user remained logged on.
- Issue 22582546: Predefined roles for job management enable users to cancel jobs and to purge job history. An attempt to create a custom role that removes the ability to purge job history also incorrectly removed the ability to cancel jobs.

Known Issue

The following issue is known to exist in version 8.6.6.4000 of GRC, and will be addressed in a future release:

- Issue 25349029: Users should be able to select any number of controls for analysis. However, when a user selects three or more access controls to be run, GRC runs only two of them. Workarounds include:
  - Identify the controls you want to analyze and run each individually, one after another.
  - Select all controls and run them.

Documentation

Documentation written expressly for release 8.6.6.4000 of GRC includes these *Release Notes* and an *Installation Guide* (part number E83508-01). Otherwise, documents written for GRC release 8.6.6.1000 apply also to release 8.6.6.4000. These documents include user guides for GRC itself as well as AAGC, ETCG, EGRCM, and GRCI; and implementation guides for GRC security, AACG, ETCG, and EGRCM.

Installation and Upgrade

You can install GRC 8.6.6.4000 only as an upgrade from version 8.6.6.3000.
Be sure to back up the transaction ETL repository and GRC schema from version 8.6.6.3000 before you upgrade.

If you use CCM, after the upgrade you must complete the following procedures in the order indicated:

- Perform access synchronization on all data sources used for AACG analysis. (Synchronization is a process that copies data from business applications to GRC for analysis by models and controls. Ordinary synchronization updates GRC with records that are new or have been changed since the previous synchronization job.)
- Perform a graph rebuild on all data sources used for ETCG analysis. (A graph rebuild is a comprehensive form of synchronization. Available only to ETCG, it discards existing data and imports all records for all business objects used in all existing ETCG models and controls.)
- Run all controls that compile data for user-defined objects (controls for which the result type is “Dataset”).
- Run all models and all controls that generate incidents (controls for which the result type is “Incident”).

Note: You may upgrade through several releases (for example, from version 8.6.6.1000 to 8.6.6.2000 to 8.6.6.3000 to 8.6.6.4000). If so, synchronize access data, rebuild the graph for transaction data, and run controls and models only once, after the final upgrade is complete.

As you upgrade to GRC 8.6.6.4000, 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 the appropriate one of the following values:

- grc.ear: `b314c38f0a5834a33ddef4d22ad66376`
- grc.war: `16b10d0257cf3254f6ff8fc9745e7fd8`

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