Oracle® Enterprise Governance, Risk and Compliance

Release Notes

Release 8.6.6.8000

Part No. E93717-01

February 2018

ORACLE

Oracle Enterprise Governance, Risk and Compliance Release Notes

Part No. E93717-01

Primary Author: David Christie

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 8.6.6.8000 resolves the following issues:

- Issue 27471915: AACG analysis may be "preventive," meaning that access controls uncover SOD conflicts at the moment a person's access assignments change. Depending on how a control is configured, preventive analysis may allow access, prevent it, or suspend it pending approval. ("Preventive analysis" is also called "user provisioning.")

  User provisioning jobs did not work as expected when multiple requests were submitted at once or within a short time interval.

- Issue 27403490: When preventive analysis suspends access assignments, a reviewer approves or rejects them in a Manage Access Approvals page. After a

user successfully approved two assignments, an attempt to review a third assignment produced a message stating that all incidents (control violations) may not have been displayed, and recommending a new control analysis. That resulted in the Manage Access Approvals page becoming unresponsive, and in subsequent user-provisioning jobs generating errors.

- Issue 27261765: After an upgrade from version 8.6.5.8000 to 8.6.6.6000, an attempt to use the Manage Results page generated an error stating that the connection to the server had failed.
- Issue 27061887: In version 8.6.6.6000, user-provisioning jobs took excessive time to run.
- Issue 26910377: An attempt to connect GRC to an E-Business Suite database enabled with Real Application Clusters (RAC) generated an error.
- Issue 26305008: The revision date of an access incident was updated with each new run of the control that had generated the incident, even if the new run did not change the existing incident.
- Issue 26275950: An attempt to search among incidents for those last updated by a specific user produced no results, even though incidents updated most recently by that user were known to exist.
- Issue 26044226: A Data Migration utility uploads operational data to an EGRCM instance. The procedure involves generating an import template and updating the template with new data. The template may include data already existing in the EGRCM instance from which the template is generated. An attempt to generate such a template omitted data concerning existing issues, remediation plans, action items for processes, assessments, and definitions of relationships among objects.
- Issue 25540539: A global condition defines exclusions from access analysis that apply to all AACG models and controls. It consists of filters that define conditions under which records are to be excluded. An In condition selects records containing a value that match any in a set of values you specify. An attempt to create such a filter caused the application to hang.
- Issue 25348586: A global-condition filter may select records to be excluded from analysis if a role assignment has passed its end date. Such a filter improperly excluded records of responsibilities included in the role, but also available to a user from another role.
- Issue 24706387: Each management page includes a grid that displays summary information about items on which the page focuses. You can search among the items in a grid, and you can save search parameters for reuse. A saved search did not return correct results in the Manage Controls page.
- Issue 24682661: A simulation previews the effects of changes you might make in your security model to resolve incidents identified by AACG controls. It consists of remediation steps, each of which hypothesizes the removal of an access point from a role hierarchy. Incidents involving that access point (reached from within that hierarchy) would therefore be resolved. Within a simulation, a Controls grid should, but did not, list controls affected by remediation steps and, for each, counts of violations that actually exist and would exist if remediation steps

were executed. (The simulation did show appropriate results for users and roles affected by the remediation steps.)

Documentation

Documentation written expressly for release 8.6.6.8000 of GRC includes these *Release Notes* and an *Installation Guide* (part number E93718-01). Otherwise, documents written for GRC release 8.6.6.1000 apply also to release 8.6.6.8000. 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 8.6.6.8000 only as an upgrade from version 8.6.6.7000. Be sure to back up the transaction ETL repository and GRC schema from version 8.6.6.7000 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. 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 8.6.6.8000, 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: `2371a648edd09a76b87a50f25f844f0b`
- grc.war: `877307c7f4bb4e68e904f1000483a991`

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