Oracle® Enterprise Governance, Risk and Compliance

Release Notes

Release 8.6.6.3000

Part No. E80458-01

October 2016

ORACLE

Oracle Enterprise Governance, Risk and Compliance Release Notes

Part No. E80458-01

Primary Author: David Christie

Contents

Release Notes 1

Resolved Issues 1

Documentation 3

Installation and Upgrade.....3

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 8.6.6.3000 resolves the following issues:

- Issue 24369768: EGRCM processes, risks, and controls may be subject to review and approval workflows as they are created or edited. They may also be included in assessments, in which they are evaluated for certification, audit, design review, or other purposes. A not-yet-approved control was available for inclusion in an assessment, although it should not have been.
- Issue 23636565: During an EGRCM assessment, an attempt to select records in a Review Prior Results page generated an error.
- Issue 23629204: AACG analysis may be "preventive," meaning that access controls are evaluated at the moment a person is assigned new access. Depending on

the “enforcement type” of an access control, preventive analysis may allow access, prevent it, or suspend it pending approval. In that last case, users review approval requests in a Manage Access Approvals page. However, this page did not show all the pending requests that should have appeared.

- Issue 23621739: As you run reports, you can select parameter values that focus the results on records that match those values. An attempt to save a set of parameter values for reuse generated an error.
- Issue 23620053: In AACG, a global condition is a set of filters that select records to be excluded from SOD analysis by all access models and controls on a given datasource. In addition, a parallel processing feature may enable GRC to run multiple jobs, including access-control analysis, simultaneously.

  When parallel processing was enabled, AACG generated incidents that should have been excluded by global conditions involving user or responsibility end dates in an Oracle E-Business Suite datasource. Also, an Access Incident Details Extract report included records of the incidents that should have been excluded.
- Issue 23539863: When parallel processing was enabled in GRC, preventive enforcement jobs generated errors.
- Issue 23492147: GRC automatically approved an access request under these circumstances: An access request with no end date was rejected in the Manage Access Approvals page. The request was resubmitted from Oracle E-Business Suite with a future end date. (A record of the approved request appeared in the Administer Access Approvals page.)
- Issue 23230888: Users should be able to select a Personalize option to customize saved sets of report parameters, for example selecting a default set for each report. An attempt to use the Personalize option with the Risk Control Matrix report generated errors.
- Issue 23223380: AACG control analysis required 24 hours to run.
- Issue 22909948: After an upgrade, ETCG ran slowly. In particular, models and controls that included user-defined objects (UDOs) ran slowly. A UDO is a set of data returned by an access or transaction control that is used as if it were a business object in another transaction model or control.
- Issue 22907749: Transaction models that included UDOs ran slowly.
- Issue 22766284: An EGRCM control may have a test plan, for use during an assessment in verifying that the control effectively mitigates risk. The plan consists of instructions, which in turn consist of steps. When an assessor completed a step by entering a response of 1,000 or more characters, other steps would not accept responses.
- Issue 22593382: An approval or rejection of an access request in the Manage Access Approvals page should set a Last Updated By value to the ID of the user who completed the action, and a Last Updated Date value to the date when the action occurred. Neither value was set correctly in the GRC database.
- Issue 21938265: To configure security, users may create roles, either from scratch or by copying predefined job or duty roles and editing the copies. When functionality to edit models was deleted from a copy of a Manage Access Models duty role, model-export functionality was also inappropriately removed.

- Issue 21615529: In AACG, conditions to exclude records from analysis may be global or may be specific to a model. In either case, condition filters may use a Contains operator. It excludes records in which an attribute value contains any in a specified set of text strings. If a condition included two Contains filters, and one of them was based on the User Name attribute, model analysis applied the first condition, but not the second.
- Issue 21183192: AACG preventive analysis requires that a preventive enforcement agent (PEA) be installed in the Oracle E-Business Suite datasource subject to access models and controls. GRC and PEAs may be installed with Secure Sockets Layer (SSL) enabled. If so, preventive analysis failed, generating a CA Server Unreachable error.
- Issue 19931793: When parallel processing was enabled in GRC, performance was poor for preventive enforcement jobs.

Documentation

Documentation written expressly for release 8.6.6.3000 of GRC includes these *Release Notes* and an *Installation Guide* (part number E80459-01). Otherwise, documents written for GRC release 8.6.6.1000 apply also to release 8.6.6.3000. 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 8.6.6.3000 only as an upgrade from version 8.6.6.2000. Be sure to back up the transaction ETL repository and GRC schema from version 8.6.6.2000 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 datasources used for AACG analysis. (Ordinary synchronization updates GRC with data for records that are new or have been changed since the previous synchronization job.)
- Perform a graph rebuild on all datasources 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). 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 8.6.6.3000, 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: `83c045db2509d3d9e8afc0c15ce8997b`
- grc.war: `0877227a657c3fde8bbc492db52a82f6`

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