Oracle® Enterprise Governance, Risk and Compliance

Release Notes

Release 8.6.6.2000

Part No. E76912-01

June 2016

ORACLE

Oracle Enterprise Governance, Risk and Compliance Release Notes

Part No. E76912-01

Copyright © 2016 Oracle Corporation and/or its affiliates. All rights reserved.

Primary Author: David Christie

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

The software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

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

Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

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.

Business Object Updates

Version 8.6.6.2000 updates one business object:

- Issue 23176409: Data synchronization failed when applied to a Territory business object for an Oracle E-Business Suite 12.2.4 datasource. Resolution of this issue required the removal of an attribute called Region Identifier.

  If you use the Territory.Region Identifier attribute in a transaction model, remove the filter that cites it from the model. If you use the Territory.Region Identifier attribute in a control, inactivate the control and create a new one from a model that does not use the attribute.

  A business object is a set of related data fields from a datasource (business application), and an attribute is one field within the set. Data synchronization is

a process that updates either user-access data for access models and controls, or data for all the business objects selected by transaction models and controls.

Resolved Issues

Version 8.6.6.2000 resolves the following issues:

- Issues 23601685 and 23040365: In AACG, a global condition is a set of filters that select records to be exempted from SOD analysis by all access models and controls on a given datasource. In release 8.6.6.1000, specific global conditions were not working.
- Issue 23063876: AACG analysis may be "preventive," meaning that access controls are evaluated at the moment a person is assigned new access. For preventive analysis to work, you install a preventive enforcement agent (PEA) in each instance of a business application subject to access analysis.

  For GRC 8.6.6.1, the PEA-installation procedure included a new setting designed to support multi-org access control (MOAC) in release 12 of Oracle E-Business Suite. The new setting was not documented and, if set improperly, could produce incorrect results for models that included any condition related to MOAC.

  If you have set up MOAC in an EBS instance, then as you install the PEA, you should select Yes in response to an "Enable MOAC?" prompt. Select No if you have not set up MOAC in your EBS instance. The default value is No. If you want to change that setting, you must reinstall the PEA. However, if you are unaffected by this issue, you need not reinstall the PEA.
- Issue 22895208: During an attempt to edit the hierarchical relationships of values in a perspective, nodes disappeared from their region of the Edit Perspective Hierarchy page.

  A perspective is a set of related, hierarchically organized values. You assign individual perspective values to processes, risks, and controls in EGRCM, or to models, controls, and incidents (control violations) in CCM. These assignments are instrumental in securing user access to data and in identifying users who can resolve CCM incidents.
- Issue 22830355: The Access Violations Within a Single Role (Intra-Role) Report identifies each role that by itself grants conflicting privileges, so that the role cannot be assigned to any user without a conflict occurring. As a parameter for the report, you can select controls that define the conflicts to be considered. The report generated an error if the number of controls exceeded 25.
- Issue 22814341: In EGRCM, a test plan provides instructions that a user follows to determine whether a control effectively addresses a risk. From the page to create or edit a control, a user may launch pages to view, create, or edit test plans for that control. An attempt to exit from these test-plan-management pages generated an error.
- Issue 22814322: When a user opened a page to view or work with a test plan, links disappeared from the Navigator.

- Issue 22810299 and 23322119: In AACG, a control-analysis job incorrectly reset the creation dates and last-updated dates of incidents generated before the job ran.
- Issue 22650280: E-mail notifications of access-approval requests were sent to users whose roles did not grant authority to act on the requests.

  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. They are entitled to do so if their roles specify perspective values that match "result" perspective values selected for the control that caused access to be suspended. (Their roles must also include a privilege to review approval requests.) Some users received e-mail notifications of approval requests even if their roles did not include matching perspective values.
- Issue 22227303: If a preventive analysis job were canceled, no other jobs could be run.
- Issue 22067922: The Access Violations Within a Single Role (Intra-Role) Report and the Intra-Role Violations by Control Report both returned false-positive results. In each report, access points within a single entitlement were incorrectly evaluated as conflicting.

  In AACG, an access point is a role, privilege, or other object that grants users the ability to view or manipulate data in a business application. An entitlement is a set of access points. An access control may set an entitlement in conflict with another entitlement. If so, any access point in one entitlement would conflict with any access point in the other. Within either single entitlement, however, access points have an OR relationship, and do not conflict with one another.
- Issue 21674304: Distinct database schemas support GRC and GRCI. The Data Analytics (DA) schema, which supports GRCI, is refreshed by the GRC schema. However, a refresh did not populate some incident columns in the DA schema, even though data existed in corresponding columns of the GRC schema.
- Issue 21636834: Transaction models generated an error when each used the business object called Customer, one model created custom attributes for that object, and the other defined a filter that set an attribute of the object equal to itself.

  A transaction model consists of filters. Each specifies an attribute of a business object, then selects records in which values for that attribute satisfy a condition you define. A filter can use an equals condition to set an attribute of an object equal to itself. The result would be groups of records, in each of which the attribute equals a specific value.
- Issue 21084735: GRC provides roles that may be granted to its users. Viewer roles should grant access to view data, but not to create or modify it. In EGRCM, a Control Viewer role improperly provided the ability to add comments to controls.
- Issue 20361238: In Manage Results pages of the user interface, certain details were missing from records of closed incidents. In the Access Incident Details Extract Report, no records of closed incidents appeared.

- Issue 20068418: When the Payables Invoice business object was used in a model, any numeric model result of seven or more digits appeared in scientific notation. This was true both for results displayed in Manage Results pages and in exported results.
- Issue 17744346: When perspective descriptions were updated, and the DA schema was subsequently refreshed, the updated descriptions did not appear in the DA schema.

Documentation

Documentation written expressly for release 8.6.6.2000 of GRC includes these *Release Notes* and an *Installation Guide* (part number E76925-01). Otherwise, documents written for GRC release 8.6.6.1000 apply also to release 8.6.6.2000. 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 8.6.6.2000 only as an upgrade from version 8.6.6.1000. Be sure to back up the transaction ETL repository and GRC schema from version 8.6.6.1000 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 8.6.5.9500 to 8.6.6.1000 to 8.6.6.2000). 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 8.6.6.2000, 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: `785e38b167c6bfcd1c26e72ab0ddf522`
- grc.war: `f6cfd5f7eacfefc88deb301279a3f266`

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