Oracle® Enterprise Governance, Risk and Compliance

Release Notes

Release 8.6.5.5000

Part No. E57010-01

September 2014

ORACLE

Oracle Enterprise Governance, Risk and Compliance Release Notes

Part No. E57010-01

Primary Author: David Christie

Contents

Release Notes

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 run within business applications to uncover segregation of duties (SOD) conflicts and transaction risk. The applications are two in a set 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.
- 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

Business objects provide data for analysis by CCM models, continuous controls, and global conditions. A business object is, in effect, a set of related fields from a datasource (instance of a business application), and an attribute is one field within the set.

The *Oracle Enterprise Transaction Controls Governor Implementation Guide* for version 8.6.5.1000 published lists of business objects delivered with ETCG for Oracle E-Business Suite 12.1, Oracle E-Business Suite 11.5.10.2, and PeopleSoft Enterprise Financials 9.1.

Subsequently, the following additions were made:

- In release 8.6.5.4000, an attribute called Line: Operating Unit ID was added to the Purchase Order business object for Oracle EBS 12.1.

- In release 8.6.5.5000, three business objects are added for Oracle EBS 12.1:

Business Object	Type	Category
Payables Audit Rules	Financials	Operational (Master Data)
Approval Management Engine Rules	Financials	Operational (Master Data)
Job Definitions	Human Capital Management	Operational (Master Data)

Resolved Issues

Issues resolved by version 8.6.5.5000 include the following:

- Issue 19517264: In the Manage Controls page, a search produced a maximum of 25 controls, even when a greater number of controls satisfied search parameters.
- Issue 19460898: An access control may contain conditions — filters that select records to be excluded from analysis by the control. A condition filter may use a Not In operator to identify a specific set of values for an attribute of a business object. Depending on further configuration, records containing values not included in that set would be excluded from or included in analysis.

  When controls containing such filters were exported from one GRC instance and imported into another, the values specified for the Not In operator were lost. For these controls, counts of incidents (records of control violations) differed in the source and destination instances.
- Issue 19455836: A global condition consists of one or more filters that select records to be excluded from analysis by all access models or controls evaluated on a given datasource. If a global condition contained a filter that used the Not In operator, was exported from a GRC instance, and was imported into another, then as was the case for control-level conditions, attribute values specified for the operator were lost.
- Issue 19442223: AACG analysis may be "preventive," meaning that access controls are evaluated at the moment a person is assigned new access. Depending on how a control is configured, it may suspend access pending approval.

  AACG users review suspended assignments in a Manage Access Approvals page. It presents business-application users and the roles provisionally assigned to them. A Preview option should show incidents for each assignment the AACG reviewer approves. If the reviewer rejected any role assignment but approved others, the Preview option failed to display incidents that applied to the approved assignments.
- Issue 19367107: A perspective is a set of related, hierarchically organized values. In the CCM module, users may assign individual perspective values to individual models, controls, or incidents, establishing a context for each. A perspective may be configured to be required — at least one value must be assigned to each eligible object. If so, global conditions could not be saved. GRC expected a value for the required perspective to be assigned to the global condition, even though there is no way to assign a perspective value to a global condition.

- Issue 19365529: The Access Incident Details Extract Report should list incidents generated by specified access controls. When run from Report Management, the report did not provide data for controls whose names contained trailing spaces. (When run "contextually" — from the Manage Results page — the report did provide data for these controls.)
- Issue 19337670: Data synchronization is a process that copies data from a data-source into GRC for analysis by models and controls. After an upgrade to GRC 8.6.5.1645, access synchronization ran excessively slowly.
- Issue 19326254: The Intra-Role Violations by Control Report lists access controls that generate conflicts between privileges granted within a role or responsibility. In release 8.6.5.3029, the report displayed no results for a control that generated more than 10,000 incidents.
- Issue 19310357: The Access Violations Within a Single Role (Intra-Role) Report lists roles for which access controls generate intra-role conflicts. In version 8.6.5.3029, the report displayed no results for a control that generated more than 10,000 incidents.
- Issue 19297128: The Access Approvals Report displays records of role assignments in business applications that were suspended, prevented, or allowed by AACG preventive processing. In version 8.6.5.3029, the Last Updated By column in the report did not correctly identify the user who approved or rejected an access request.
- Issue 19270208: GRC release 8.6.5.5000 is confirmed to be certified for Oracle Database release 11.2.0.4.
- Issue 19270068: Global conditions may use a Within Same Ledger/Set of Books attribute of condition business objects. Depending on configuration, it should identify conflicts (as defined by models or controls) that occur only within or only across individual ledgers or sets of books. However, when a global condition was created to use this attribute (in varying configurations), models that should have returned results did not.
- Issue 19227734: Perspective values may be associated with data roles, which are included in job roles that are assigned to users. A user should have access only to data associated with the perspective values included in his data roles. However, in the Manage Access Approvals page, users could see access requests associated with perspective values not included in their data roles.
- Issue 19221429: An error occurred during upgrade from GRC 8.6.4.8500 to GRC 8.6.5.1616.
- Issue 19218007: To use GRC with applications other than Oracle E-Business Suite or PeopleSoft, one would need to create a custom connector, which uses ETL technology to provide application data in a format that GRC recognizes. A custom connector could support access conditions based on access point names, but did not support conditions based on other values. (An access point is an object, such as a menu or function, that enables users to view or manipulate data in a business application.)
- Issue 19183301: In AACG, an entitlement is a configured set of access points. An AACG model defines conflicts among access points, and may use entitle-

ments to do so. Attempts to navigate in the Manage Access Entitlements page, or to create new entitlements, generated errors.

- Issue 19129954: If a user were assigned a role designed to give view-only access to transaction models, that user's attempt to select Continuous Control Management in the Navigator resulted in an error.
- Issue 19072602: When preventive analysis is in force, AACG rejects the assignment of duties that violate a control whose enforcement type is Prevent. If multiple users were assigned Oracle E-Business Suite responsibilities within a brief time, and any assignment violated a Prevent control, then all were rejected. If responsibilities were reassigned to users for whom the assignment should not have violated a Prevent control, results were inconsistent when performed for multiple users.
- Issue 19064791: After an upgrade from GRC 864.8329 to 865.1645, a user imported models and controls from a development instance, ran synchronization successfully, but encountered errors during control analysis.

Known Issues

The following issues are known to exist in version 8.6.5.5000 of GRC, and will be addressed in a future release:

- Issue 19461143: GRC fails to start if worklist, notification, or watchlist data is bad. (A worklist is both a record of a task that is assigned to the user who has logged on to GRC, and a link to the page on which the task can be completed. A notification is a record of a task in which the user has an interest, but on which he need not act. A watchlist is a summary of worklist entries.)
- Issue 19452051: When a global condition contains a filter that uses the GL: Data Access Set attribute, and preventive analysis of a control generates approval requests in the Manage Access Approvals page, those requests are improperly auto-approved.
- Issue 19445327: In the Manage Access Entitlements page, searches result in an error if Effective Date, Revision Date, Created On, or Last Updated Date is used as a search parameter.
- Issue 19431269: Incident notifications are sent to users whose roles should not give them access (because their roles are associated with perspective values that do not match the values associated with the incidents).
- Issue 19357249: An access model may return false negatives under the following conditions: In Oracle E-Business Suite, a menu is assigned a type value other than Standard. In GRC, an access model includes a filter to select users granted that menu. A condition filter (either within the model or within a global condition) uses the Menu Function Grant Flag attribute or the Submenu Grant Flag attribute.
- Issue 19154005: Distinct database schemas support GRC and GRCI. The Data Analytics (DA) schema, which supports GRCI, is refreshed regularly by the GRC schema. When CCM incidents are purged in GRC, and the DA schema is subsequently refreshed, the purged incidents continue to appear in GRCI reports.

Documentation

Documentation written expressly for release 8.6.5.5000 of GRC includes these *Release Notes* and an *Installation Guide* (part number E57011-01). Otherwise, documents written for GRC release 8.6.5.1000 (as well as *Release Notes* for 8.6.5.2000, 8.6.5.3000, and 8.6.5.4000) apply also to release 8.6.5.5000. 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. These documents are available on Oracle Technology Network at http://www.oracle.com/technetwork.

Installation

You can install GRC 8.6.5.5000 only as an upgrade from version 8.6.5.4000. Be sure to back up your 8.6.5.4000 transaction ETL repository and GRC schema before you upgrade to 8.6.5.5000.

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

- Perform access synchronization on all datasources used for AACG analysis. (Ordinary synchronization is incremental, collecting data only for records that are new or have been updated 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 "Incidents").

Note: You may be upgrading through several releases (for example, from version 8.6.4.7000 to 8.6.5.1000 to 8.6.5.2000 to 8.6.5.3000 to 8.6.5.4000 to 8.6.5.5000). 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 install GRC 8.6.5.5000, 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: `9159b18926524ff66b7cb53f50552aab`
- grc.war: `77c9b5da8621d565fb61befab0dfa5c9`

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