Oracle® Enterprise Governance, Risk and Compliance

Release Notes

Release 8.6.4.8000

Part No. E41915-02

August 2013

ORACLE

Oracle Enterprise Governance, Risk and Compliance Release Notes

Part No. E41915-02

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," and to run them within business applications to uncover and resolve segregation of duties violations and transaction risk. These 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. It enables users to define risks to the company's business, controls to mitigate those risks, and other objects, such as business processes in which risks and controls apply.
- 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.

User Defined Access Points

A CCM model or control consists of filters, each of which defines some aspect of risk and selects records that satisfy the definition.

In AACG, a filter may select users granted an access point to the company's applications; combinations of such filters identify users whose access might constitute segregation of duties conflicts. An access point is an object in a business application that enables a user to view or manipulate application data. In earlier versions, access points were defined by GRC. Examples include functions or responsibilities in Oracle E-Business Suite, or menus or page definitions in PeopleSoft.

Whether an access point legitimately constitutes an element of an SOD conflict may depend, however, on how the user can reach it. In PeopleSoft, for example, the Jour-

nal Entry page enables users both to enter and approve journals, so it may present a risk if a user can reach it through menus (or other components) that grant write access. However, it would not present a risk if the user reaches it through another path that provides only read access.

Thus, rather than include an access point in an access filter, one may wish to include an access path. Beginning with version 8.6.4.8000, AACG permits the creation of user defined access points (UDAP), each of which is a specific path to a seeded access point. For PeopleSoft analysis, UDAPs may incorporate not only access points, but also user preferences (properties of individual users that determine what they may do on a given page).

User Defined Objects

To specify data for analysis, CCM models and controls may cite business objects, each of which is a set of related data fields from a datasource (instance of a business application). An attribute of a business object is one field within the set.

Transaction models and controls may cite other types of objects as well: A custom object is a set of data imported from an xml file. A system generated object is data returned by certain transaction filters.

To these, version 8.6.4.8000 adds the user defined object — a set of data, returned by a CCM control, that is used as a business object. Each column in the results returned by one of these specially configured controls serves as an attribute of the object generated from the control.

Although only transaction models and controls can cite a user defined object, either an access or a transaction control can supply data to a user defined object.

A control can generate incidents (records of control violations that are reviewed by result investigators), or it can provide data to a user defined object, but it cannot do both. A user who creates a control sets a Result Type field to determine which purpose the control serves.

When it is created, a user defined object has no join relationship to other objects. As a user creates filters in transaction models, he can use a “Related to” operator to establish a join relationship between an attribute of a user defined object and an attribute of a seeded business object, a custom object, or another user defined object.

PeopleSoft User Preferences in Access Models and Controls

Although some AACG filters identify users granted access points, others define conditions, each of which exempts users or other objects from analysis. An AACG global condition may contain filters that define exemptions for all models and controls evaluated on a given datasource.

An AACG model or control may include a filter that selects users with access to a page, but to eliminate false positives, it may also include a condition that excludes those who are not authorized to perform particular actions in that page. A new Page Access Configurations business object provides values for use in such condition filters.

For 8.6.4.8000, this business object applies only to PeopleSoft, in which user preferences determine what users can do in pages to which they have access; the Page Access Configurations object consists of user-preference values. For example, a model concerned with the creation of adjustment vouchers could include a filter that selects users with access to the Create Voucher page. It could also include a condition filter to exclude those who do not have the Allow Adjustment Voucher user preference, and therefore cannot actually create adjustment vouchers even though they have access to the Create Voucher page.

In earlier GRC versions, a PeopleSoft Access Condition business object included some user-preference values. These have been removed from the PeopleSoft Access Condition object and incorporated (along with many other user-preference values) into the Page Access Configurations object.

In version 8.6.4.7000, models, controls, and global conditions may have included filters that cited user-preference values from the PeopleSoft Access Condition business object. These cannot be upgraded to version 8.6.4.8000; instead, they are removed during the upgrade and must be re-created. You can use the Access Incident Extract Report and the Control Detail Report to identify such controls. Moreover, logs list controls, models, and global conditions deleted during the upgrade.

(Page Access Configuration processing is enabled by default, but can be disabled during GRC installation. If you do not intend to use Page Access Configuration data, you can improve performance and reduce memory requirements by disabling this feature. See the *Enterprise Governance, Risk and Compliance Installation Guide*.)

Result Attribute Selection in Transaction Models

Transaction models (and controls) specify attributes to be reported as results. In earlier versions, model results automatically included all attributes cited in filters that define model logic, and these could not be removed from the results. In version 8.6.4.8000, "derived attributes" continue to be selected automatically as model results. (These are attributes that exist only as calculations performed by a model, such as sums, counts, or averages calculated by function filters.) However, a user must actively select any other attribute for inclusion among model results — even those used to define model logic.

This enables users who define models to specify the granularity of results. For example, a model may group invoices by supplier (include a filter that sets the Supplier ID attribute of the Payables Invoice business object equal to itself). It may also include a function filter that calculates a sum of invoice amounts for each supplier. The sum value, a derived attribute, is included automatically in the result set. In earlier releases, the Invoice Amount attribute would also have been included automatically, because it is used in the model logic to calculate invoice-amount sums. So that individual invoice amounts could be reported, results would necessarily include a row for each invoice. Rows would be grouped by supplier, and each would also show the sum for the supplier's invoices (and values for any other attributes selected as results).

In version 8.6.4.8000, a user may choose to include the Invoice Amount attribute among result values, in which case the results would be the same. Or he may choose to omit this attribute, in which case results would include only one row for each supplier, displaying the sum of that supplier's invoices.

Results for Transaction Models and Controls That Detect Similarity

A filter in a transaction model (or control) may select transactions in which the values of one or two attributes are similar. In most cases, values are similar if a specified percentage of their characters are the same, although dates are similar if they fall within a specified number of days of one another.

The filter collects records into groups, in each of which records meet the standard of similarity in a distinct way. For example if a Similar filter says that the values of a six-character text field must be 50 percent alike, values containing *abc* might constitute one group, and values containing *xyz* might constitute another.

A given record may qualify for more than one group. Beginning with version 8.6.4.8000, however, the default behavior is for that record to belong only to the one group in which it is most strongly similar to other values. The effect is to reduce the number of records returned by a model that uses a similar filter (or incidents returned by a control developed from such a model), because a record that could have been returned for any number of groups is instead returned only once.

You can set a Generate Results for Similar Groups advanced option to have each record belong to all groups for which it qualifies. In that case, results are reported as they had been in earlier versions.

Resolved Issues

Issues resolved by version 8.6.4.8000 include the following:

- Issue 17186477: The Transaction Incident Details Extract Report should display both summary and detailed information about incidents generated by transaction controls. In earlier versions, the report included the summary data, but not the details.
- Issue 17186315: When an AACG model specified a PeopleSoft page as an access point, the model continued to return results for a user even after that user's authorization for access to the page was deselected in PeopleSoft.
- Issue 17178889: AACG may perform preventive analysis — analyze controls as a user is assigned duties in a business application, and (in accordance with the enforcement type configured for each control) deny access to those duties, allow access, or suspend access until the assignment can be reviewed. When AACG should have suspended the assignment of an Oracle EBS responsibility to a user, it did so on the initial assignment, but failed to do so when the user's end date for the responsibility was edited, and the assignment was resubmitted.
- Issue 17050500: An access condition to exclude a PeopleSoft panel group component from analysis failed. A model containing the condition filter returned access paths including the component.
- Issue 17019089: CCM users regularly synchronize data — run processes that capture changes made in datasources in which models or controls evaluate risk. In version 8.6.4.7181, an attempt to run access synchronization generated errors.
- Issue 17005807: Synchronization should be incremental — it should create or update only records that are new or have changed since the previous synchroni-

zation. Under certain circumstances, however, GRC ran a full rather than incremental synchronization of transaction data.

- Issue 16992093: After an upgrade from GRC 8.6.3 to 8.6.4, the incident count in the later version was much higher than it had been in the earlier version, with originally accepted incidents set to Closed status and In Investigation state.
- Issue 16978370: Worklists are records of tasks that require a user's attention. In the CCM module, they are records of incidents to be investigated. GRC displays CCM worklists in the home page and the result-overview page of users assigned to investigate the incidents.

  Users may purge incidents generated by CCM controls (in the Maintenance tab of the GRC Manage Application Configurations page). If pending incidents are purged, however, the worklists that listed them continue to exist, but lead nowhere. To prevent this from happening, close the worklists before purging the incidents. One way to do this is to identify pending incidents among those you intend to purge, and resolve them to a status at which they are no longer pending. Another way is to inactivate controls that have generated pending incidents before you purge the incidents.
- Issue 16972548: After upgrade from GRC 8.6.4.6000 to 8.6.4.7000, access synchronization failed.
- Issue 16901893: GRCI dashboards displayed results only for controls that were most recently analyzed. Results for controls that had previously been displayed were dropped if the controls were not included in the most recent analysis.
- Issue 16893589: AACG users may create path conditions, each of which excludes a specific path to an access point from incident generation. After access synchronization runs, the Manage Access Path Conditions page displayed spurious path conditions (all set to Inactive status).
- Issue 16892250: A connector uses ETL technology to collect data from a business application and provide it in a format that GRC recognizes. A default connector, provided with GRC, does this for Oracle EBS and PeopleSoft instances. Custom connectors may do this for instances of other applications. For DB2 support, custom and JDBC connectors were updated for version 8.6.4.8000.
- Issue 16887894: Users may attach files to CCM incidents (or to any object in the Financial Governance module or custom modules). One type of attachment is the URL for a web site. Any number of CCM incidents may be edited at once; during such a "mass edit," a URL is the only type of attachment users may create. However, these attachments did not work. When a user saved the mass edit, then opened the page displaying details for any of the edited incidents, the URL attachment did not appear.
- Issue 16880615: GRC management and overview pages display lists of items. On each page, search features enable users to create customized lists of items. A basic search offers commonly used search parameters, while an advanced search expands the possible parameters, and enables users to add fields as parameters. An attempt to add fields to an advanced search on the CCM Manage Results page generated an error.

- Issue 16879594: In ETCG, data synchronization may be applied to individual models. However, synchronization failed for a model that used the Payables Invoice and Supplier business objects.
- Issue 16873511: A perspective is a set of related values that define a context in which GRC objects may exist. Users associate individual perspective values with individual objects, in effect cataloging them. A CCM control specifies two sets of perspective values: One applies to the control itself, and the other applies to incidents generated by the control.

  GRCI uses a Data Analytics (DA) database schema, which is distinct from the schema used by GRC itself. The DA schema did not recognize the association of perspective values to incidents and controls, and so GRCI reports returned improper results.
- Issue 16863843: "Who" attributes of business objects identify users who complete actions in target applications. An example is the Last Modified by User attribute of the Supplier business object. For PeopleSoft business objects, who attributes that could have been provided were missing.
- Issue 16844498: Transaction synchronization failed with a duplicate-key error for a model that used the Application User business object.
- Issue 16842322: In EGRCM, assessments enable appropriate users to review configured objects such as processes, risks, and controls. During an assessment of a control, comments associated with a request for more information were lost.
- Issue 16837432: After an upgrade to version 8.6.4.6169, access synchronization failed.
- Issue 16809587: Under certain circumstances, AACG models and controls could produce false-positives when run in a PeopleSoft instance. For example, incidents might be generated for users with display-only access to PeopleSoft pages, even though conditions had been created to exclude such users. After you upgrade to GRC 8.6.4.8000, synchronize data, and rerun conflict analysis in a PeopleSoft instance, you can expect some incidents to be closed automatically because they had been false positives.
- Issue 16808399: When AACG preventive analysis suspends the assignment of duties until those assignments can be reviewed, that review is completed in a Manage Access Approvals page. In it, one would select a user, then select a Preview prompt to display records of the user's access conflicts. However, selecting the Preview prompt failed, generating a communication-with-server error.
- Issue 16792837: When a user attached a file to a CCM incident, then closed and reopened the page in which incident details are displayed, the attachment was no longer available.
- Issue 16769821: Although CCM worklists constitute incidents to be investigated, each corresponds to a control, and encompasses all pending incidents generated by the control. After all incidents for a control are resolve to a status at which they are no longer pending, the worklist for that control should cease to exist. But worklists for controls remained active even when no pending incidents remained for those controls.

- Issue 16757902: In AACG, an entitlement is a set of access points; when an access filter specifies an entitlement, it selects users assigned any access point within the entitlement. However, if a model included filters that select distinct entitlements, and if those entitlements shared common access points, incidents involving those common access points were not generated.
- Issue 16756533: GRC supports parallel processing — the designation of multiple processor cores for model and control analysis. When parallel processing was engaged, preventive analysis failed when applied to an Oracle E-Business Suite instance.
- Issue 16750999: Users can implement "seeded content" — sets of CCM models and controls created by Oracle for use with specific versions of business applications. Seeded content for AACG now includes a control that identifies PeopleSoft users with the PeopleSoft Administrator role (which grants access to everything in PeopleSoft).
- Issue 16735553: A Data Migration utility enables users to upload operational data for EGRCM modules, or perspective data for the CCM module. However, attempts to upload data for EGRCM issues and remediation plans resulted in errors.
- Issue 16724643: If a user pressed the space bar while adding comments to the review of an EGRCM object, an Actions drop-down was placed in focus. A second press of the space bar automatically accepted the object.
- Issue 16706301: A transaction model that used the Purchase Order and Receipt business objects returned a set of purchase-order records, then improperly returned fewer records if the Business Unit business object was added to the model.
- Issue 16547750: Combinations of CCM model filters define a risk (for example, two filters specify two access points that in combination provide risky access). To express these relationships, users arrange filters in AND or OR relationships, which are represented by vertical or horizontal alignments of filters in a Model Logic panel. After a user modified the vertical and horizontal alignment of filters and saved changes, GRC duplicated some filters.
- Issue 16546449: Attempts to modify the vertical or horizontal alignment of filters produced a "move validation failed" error.
- Issue 16514661: Model filters may be gathered into a group to be analyzed as a logical unit. An "ungroup" feature should dissolve a group, restoring its members' individuality. In access models, however, grouped filters could not be edited or ungrouped.
- Issue 16463903: In the Properties tab of a Manage Application Configurations page, a user may enable parallel processing — designate a number of processor cores for use in evaluating models and controls simultaneously. The user would also allocate an amount of system memory for use in parallel processing.

  GRC would not necessarily accept the number of cores specified by the user. That was because each core requires a minimum amount of memory. GRC would automatically divide the user-specified memory value by that minimum amount to calculate a number of cores, and would substitute that value for the number of cores designated by the user. Each core would always use only the minimum amount of memory.

In release 8.6.4.8000, the user configuring parallel processing once again designates a number of cores and a system-memory value, but must ensure that the memory value is at least the minimum value for one core (4,096 MB) times the number of cores. GRC divides the memory value by the core value to determine the actual amount of memory allocated to each core. Both the number of cores and the memory amount specified by the user are honored, and each core may be configured to use more than the minimum amount of memory.

- Issue 16371521: An EGRCM assessment may be based on a plan, which is in turn developed from a template. For custom modules, a user creating an assessment template could, but should not have been able to, select Issue as the primary object of assessment.
- Issue 16264563: In PeopleSoft instances, most user preference values were not available for use in condition filters created for access models and controls. In version 8.6.4.8000, a new Page Access Configurations business object provides these values. (See "PeopleSoft User Preferences in Access Models and Controls," page 1-2.)
- Issue 13740447: Comments to CCM controls did not preserve line breaks.

Known Issues

The following issues are known to exist in version 8.6.4.8000 of GRC, and will be addressed in future releases.

- Issue 17283800: During an upgrade from version 8.6.4.7181, inactive path conditions are not upgraded (although active path conditions are correctly upgraded).
- Issue 17278442: You may set a "Graph Synchronization Date Limit." If so, the synchronization of certain business objects used by ETCG applies only to records created or updated on or after a date that you specify. (These are Transaction business objects, in which records are created or updated frequently, as opposed to Operational and Configuration business objects, which consist of master-data or setup records that change infrequently.) When you set a date limit (in the Manage Application Datasources page), a message instructs you to restart the application server and to synchronize all transaction datasources. Although synchronizing data is necessary, you need not restart the application server.
- Issue 17080526: GRC does not save edits to an access model filter that uses the Page Access Configurations business object.
- Issue 17075120: The Page Access Configurations business object contains duplicate values for process groups.
- Issue 17074254: When an access model includes a filter that uses the Page Access Configurations business object, an attempt to convert the model into a control generates a duplicate-record error.
- Issue 17072733: A model returns unanticipated results (no records or excessive records) if it relates an attribute of a user defined business object to an attribute of a seeded business object.
- Issue 17070943: A model that incorporates more than two business objects returns unexpected results. An invoice was created against a location of a sup-

plier with multiple locations. A model that incorporated the Payables Invoice, Supplier Site Location, and Supplier business objects should have returned a single record for that invoice, but instead returned three records, one for each location.

- Issue 17069645: In records of access incidents (in the Manage Results page), when the conflicting access point is a user defined access point, a Conflicting Access Point column should display the entire UDAP path, but instead shows only the access point that ends that path. Also, a Conflicting Access Point Type value should read "User Defined."
- Issue 17068573: In records of access incidents, a Group column displays pairs of conflicting access points assigned t a user. When a control cites an entitlement that includes a user defined access point, and the control generates more than one incident for a given user, an attempt to expand the Group column causes records of incidents to be hidden.
- Issue 17061820: In access models, conditions that cite the Page Access Configurations business object are not applied to users who are not employees.
- Issue 17029759: GRC users may be created directly in GRC, or imported from a Lightweight Directory Access Protocol (LDAP) repository. On the GRC Edit User page, the password and confirm password fields should be disabled for LDAP users. Because passwords are maintained in the LDAP repository, a password entered in GRC is ignored.
- Issue 17019585: Users without the appropriate privileges are able to run and view the Entitlement Report. (In AACG, an entitlement is a set of access points; when an access filter specifies an entitlement, it selects users assigned any access point within the entitlement. An Entitlement Report lists access points belonging to a each in set of entitlements.)
- Issue 16985257: A Manage Results page may display either a list of controls that have generated incidents, or a list of the incidents generated by those controls. In the control-summary view, users may select a variety of parameters to search for controls. A search that uses a Datasource parameter does not produce correct results.
- Issue 16930134: In EGRCM, a user may employ models to analyze "inherent" or "residual" effects of risks. One of these is an analysis model. When risk data is imported through the Data Migration utility, however, the Analysis Model field is grayed out, and users cannot designate an analysis model for imported risks.
- Issue 16914742: The Data Migration utility can upload perspectives from an xml template into GRC. However, a PerspectiveHierarchy worksheet in the template does not correctly handle trailing spaces in the names of perspective values.
- Issue 16881646: When access incidents are generated by controls that specify entitlements, the DA schema (which supports GRCI reporting) does not store entitlement information with the incidents. So entitlement data for such incidents is unavailable for GRCI reporting.
- Issue 16864262: While creating filters for access models, a user may select access points from an Access Point List popup window. This window reverses Name and Description values for PeopleSoft permission lists.

- Issue 16810567: Users may create user-defined attributes (UDA) for EGRCM controls, risks, processes, or other objects — information added to a given object to extend its definition. A UDA may incorporate lookup data — a set of values from which a user may select. In such cases, GRCI reports incorrectly display a lookup key rather than the lookup value.
- Issue 16810212: When the DA schema is updated, UDA values are not correctly reflected in GRCI reports.
- Issue 16799263: A user assigns status to a CCM incident, but GRC also assigns it a state. The state is determined not only the status a user chooses, but also by whether a user who selects a status saves or submits the selection. A save should not change the state, while a submission may advance the incident to a new state. However, state is changing even when a new status is merely saved.
- Issue 16772443: CCM model results may be exported to an Excel file. However, GRC creates a trailing space in every field of the export file.
- Issue 16694189: EGRCM users may identify issues with processes, risks, controls, or other objects, and may create remediation plans to address those issues; each plan comprises a set of tasks. Users may add comments to remediation plans and tasks, but GRCI reports do not display those comments.
- Issue 16658451: The display of access incident details includes an Incident Information field, in which GRC reports the path through which a user, assigned access points that a control defines as conflicting, can reach one of those access points. For PeopleSoft incidents, this field does not display paths in the same way as PeopleSoft itself does, in some cases using what PeopleSoft would consider the names of objects, and in other cases what PeopleSoft would consider to be their descriptions.
- Issue 16556598: GRC users are assigned job roles, which consist of duty roles and data roles. Duty roles enumerate privileges to use application features, while data roles identify sets of data a user may work with. A View Jobs duty role not only provides read access to the GRC Manage Jobs page, but inappropriately enables users to cancel and purge jobs as well.
- Issue 14838940: For each control defined in EGRCM, users may create test plans. These document steps to be followed in determining whether the control is effective. A user executes a test plan while completing an assessment of the control to which the plan is attached. An attempt use the Data Migration utility to import a test plan with assessment UDAs results in an error.

Beta Features

GRC incorporates features that are considered “beta.” These include the ability to relate objects in one EGRCM module to objects in another, to store attachments in Oracle WebCenter Content rather than the GRC database, and to build ETCG models and controls that use patterns other than Benford and Mean. Because these are beta features, they are not documented in official user documentation. They are, however, documented in white papers that are available upon request.

Support Suspended for Internet Explorer 9

Some GRC elements depend on services provided by the web browser in which GRC is displayed. Recent automatic updates to services provided by Microsoft Internet Explorer 9 (IE9) cause certain GRC pages not to perform as desired. An example of such an update is the desupport of Adobe SVG Viewer within IE9. Therefore, GRC support for IE9 is deferred until the discrepancies can be addressed. GRC continues to support the use of IE 8.*x* or FireFox 17.

Installation and Upgrade

You can install GRC 8.6.4.8000 only as an upgrade from version 8.6.4.7000 — specifically, build 7181. (Version 8.6.4.7000 is itself an upgrade from 8.6.4.6000, which is an upgrade from 8.6.5000, which can be installed independently from previous releases.)

The upgrade to version 8.6.4.8000 purges all ETCG incidents, because enhancements to this version substantially alter the way transaction incidents are generated and stored. After you install version 8.6.4.8000, run transaction controls to generate a fresh collection of incidents. The upgrade to version 8.6.4.8000 also purges AACG incidents related to controls that could not be upgraded — those that cited user-preference values from the PeopleSoft Access Condition business object.

Be sure to back up data for your 8.6.4.7000 instance before upgrading to 8.6.4.8000.

As noted earlier, GRCI uses a Data Analytics (DA) database schema, which is distinct from the schema used by GRC itself. You can run GRCI only if you create its DA schema as you install GRC version 8.6.4.5000. (If you upgrade to GRC 8.6.4.5000, you may either create a new DA schema if none yet exists, or upgrade an earlier instance of the DA schema.) You must then connect the DA schema to GRC 8.6.4.5000, and reconnect it to subsequent, upgrade-only releases (8.6.4.6000, 8.6.4.7000, and 8.6.4.8000) as they are installed.

Thus, if you expect to use GRCI with GRC 8.6.4.8000, but have not yet installed GRC 8.6.4.5000, be sure to create and connect the DA schema for 8.6.4.5000, and to reconnect it for each subsequent release, even if you do not intend to use GRCI until 8.6.4.8000. (Connectivity is configured in the Analytics tab of a Manage Application Configurations page. See the *GRC Installation Guide*.)

As you install GRC 8.6.4.8000, 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 a value published in these *Release Notes*. Your checksum value should match one of the following:

- grc.ear: `54e117a48f9a3d4abbd2e87889c2b5f1`
- grc.war: `d10f562f35661996bcaeb29677bc161e`

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