Oracle® Enterprise Governance, Risk and Compliance

Release Notes

Release 8.6.5.1000

Part No. E52267-01

March 2014

ORACLE

Oracle Enterprise Governance, Risk and Compliance Release Notes

Part No. E52267-01

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," 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.
- 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.

CCM Issues

A CCM model defines risk logic and may return temporary results. A continuous control is based on a model, adopting its risk logic typically to generate permanent incidents — records of control violations. GRC 8.6.5.1000 resolves the following issues, which apply both to AACG and ETCG:

- Issue 17540618: In build 8.6.4.9292, an attempt to create an access or transaction control generated an error.
- Issues 17419852 and 17577638: Notifications by email (configured in the Notification tab of the Manage Application Configurations page) were not sent when continuous controls were created, or in certain instances when incidents were generated.

- Issue 16867754: Each control designates one or more result investigators — users who investigate incidents generated by the control. In the Incident view of the CCM Manage Results page, the result investigator was not included in the data that could be presented about each incident.
- Issue 18301543: CCM control-analysis jobs reset last-update dates in records of incidents, even though nothing about the incidents had changed. This potentially overwrote dates on which result investigators had edited incident records.
- Issue 16812269: Users may purge incidents generated by CCM controls (in the Maintenance tab of the GRC Manage Application Configurations page). An attempt to purge both access and transaction incidents resulted in only the transaction incidents being purged. An access purge job could purge only the incidents generated by a single control.
- Issue 16799263: A result investigator assigns status to a CCM incident, but GRC also assigns it a state. The state is determined not only by the status the investigator selects, but also by whether the investigator saves or submits the status selection. A save should not change the state, while a submission may advance the incident to a new state. However, state was changing even when a new status was merely saved.
- Issue 16772443: CCM model results may be exported to an Excel file. However, GRC created a trailing space in every field of the export file.

ETCG Issues

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.

Moreover, a CCM model or control consists of filters. Each specifies an attribute of a business object and compares values for that attribute with a fixed value or with the values for another attribute. Each includes a "condition" that determines how values are compared, and returns records for which the comparison is true.

GRC 8.6.5.1000 resolves the following issues, which apply specifically to ETCG:

- Issue 18126129: A transaction model did not return expected results when it used the Is Not Related To condition to filter data from the Expense Report and Expense Report Policy Violation business objects.
- Issue 18091609: A relationship should exist between Bank Statement and Business (Operating) Unit business objects, but did not. This prevented them from being used together in a transaction model.
- Issue 17897559: An ETCG model that used a Purchase Order business object did not capture all purchase order lines that existed in an Oracle EBS source instance.
- Issue 17882815: An ETCG model produced no results when it cited the Purchase Order Line Location and Requisition business objects against a PeopleSoft Financials 9.1 instance. (Models that used either of these business objects individually did produce results.)

- Issue 17768325: A transaction model used the Journal Entry business object to search for duplicate journal entries; an attempt to run the model failed.
- Issue 17593709: An attempt to use the Journal Entry and Journal Auto-Reversal business objects in a transaction model produced no results.
- Issue 17592524: When a transaction model filter used the Created by Name attribute of the Journal Entry business object, the filter did not work as expected. When the attribute was selected for inclusion among model results, no results were returned for it.
- Issue 17546295: To support a transaction model intended to check whether invoices have the correct withholding tax, an attribute called "Distributions: Withholding Group Identifier" was added to the Payables Invoice Details business object.
- Issue 17006272: Code Combination ID values were not available to transaction models that used the Payables Invoice Details business object.
- Issue 16802405: So that currencies could be converted to US dollars in transaction models, a relationship was mapped between the General Ledger Daily Rates business object and the Payables Invoice business object.
- Issue 17721850: The import of a custom object failed if it contained 300 or more records. (A custom object is a set of data imported from an xml file, which may be used in a transaction model as if it were a business object.)
- Issue 18119095: A transaction model or control may cite a user defined object — a set of data returned by a specially configured access or transaction control. When a user defined object was developed from a control that was in turn developed from an imported model, and was then used in another imported model, that model improperly returned no results.
- Issue 18083348: An ETCG model that worked in GRC 8.6.4.8000 (build 8322) no longer worked after an upgrade to 8.6.4.8800 (build 9710).
- Issue 17546901: The Count function did not return expected results in a transaction model intended to compare counts of total invoice lines and purchase order line IDs per invoice.
- Issue 17025621: The Is Not Related To condition, available for use in transaction-model filters, should mimic the "not exists" operator in SQL.
- Issue 16997841: An attempt to create a custom attribute failed. The custom attribute was based on a date attribute and was for use in a ETCG model.
- Issue 17868967: A seeded transaction model, "1200 TXN: Receivables Debit Memo – Amount Remaining EBS R12," did not produce results for "Receivables Invoice.Line: Remaining Line Amount Due" and "Receivables Invoice.Line: Original Line Amount Due."
- Issue 17544667: A seeded transaction model, called "20000 RA" and intended to check for duplicate invoice payments, generated a disk-space error and, when disk space was increased, took excessive time to run.
- Issue 16739547: An attempt to run transaction controls generated an error.

AACG Issues

In AACG, an access point is an object in a business application that enables a user to view or manipulate application data, and an entitlement is a set of access points. An AACG model filter may select users granted a specific access point, or any access point in an entitlement. Combinations of such filters identify users whose access might constitute SOD conflicts. GRC 8.6.5.1000 resolves the following issues, which apply to AACG:

- Issue 17628711: When GRC was upgraded to version 8.6.4.8000 (build 8322), and access synchronization and control analysis were run, incidents that had been accepted and remediated in the earlier version were wiped out, and were replaced by incidents at the Assigned status.
- Issue 17570341: AACG filters, particularly those that specify entitlements, may require the analysis of a large number of access-point combinations, even if the number of filters is not large. Performance suffers when the number of combinations is excessive. Because of enhancements to GRC 8.6.5.1000, this limit is much larger than it had been. (The recommended maximum is 18,000.)
- Issue 16766927: In a Manage Access Entitlements page, the status of individual access points within a selected AACG entitlement was displayed as 1 or 0. Access points within an entitlement no longer display a status; they are presumed to be active if the entitlement itself is active.
- Issue 17596952: While creating a filter for an access model, a user may search for access points or entitlements by selecting name, description, datasource, or type values in an Attribute Values List window. When the user attempted to sort or search for values, GRC was unable to complete fetching data for the Attribute Values List.
- Issue 16864262: If a user selected PeopleSoft Permission List as the type in the Attribute Values List window, the window reversed the values displayed for name and description.
- Issue 16583575: In a PeopleSoft environment, some access points were not available for use in access models and entitlements.
- Issue 17408721: A seeded model — "5870 Approve Purchase Orders & Create Purchase Orders EBS R12" — relied on entitlements that contained inappropriate access points.
- Issue 17816727: A global condition sets limits on the conflicts identified by all access models or controls evaluated on a given datasource. A grid on a Manage Access Global Conditions page should list all such conditions. However, it displayed up to 50 rows; no "next page" link existed to enable users to view subsequent rows.
- Issue 17637874: A global condition used the In operator to select a set of menu names that were excluded from access analysis. An attempt to add menu names to the set resulted in already-selected names being overwritten.
- Issue 17783191, 17657821, and 17616645: While creating filters for global conditions, a user may select values from an Attribute Values List window. When the user attempted to sort or search for values, GRC was unable to complete fetching data for the Attribute Values List.

- Issue 16218004: Within an access model, control, or global condition, a filter may specify "within same operating unit," restricting analysis to conflicts that occur within, but not across, individual operating units. This filter did not produce expected results.
- Issues 16538882 and 16556004: In access condition filters, the "within same operating unit" and "within same ledger/set of books" conditions did not correctly recognize multi-org access control (MOAC) processing logic in Oracle EBS instances. OEBS security profile, data access set, and other options may be assigned at the user, responsibility, or site level. For each option, user is the first-priority selection. A responsibility value applies to users for whom no selection is made. The site value applies to responsibilities and users for which no selections are made. In version 8.6.5.1000, AACG analysis respects this hierarchy.
- Issue 16523440: The page in which a user would edit an access control did not open or was truncated (depending on browser).
- Issue 17836903: An access control, and the incidents it generated, continued to appear on the Manage Results page even after the control was inactivated in the Manage Controls page.
- Issue 17530996: An access control generated incidents for responsibility assignments in Oracle E-Business Suite that had passed their end-dates.
- Issue 17464411: A global condition in which filters used the Contains condition did not exclude the records it specified from access analysis.
- Issue 17896735: AACG preventive enforcement applies access controls as each user is assigned responsibilities in Oracle E-Business Suite or roles in PeopleSoft. However, when the Effective From Date for a responsibility assignment in Oracle EBS was set to a future date, AACG inappropriately auto-approved the assignment.
- Issue 17819128: A Manage Access Approvals page displays records of role assignments that have been suspended through AACG preventive enforcement. A Preview button should enable users to view details of such assignments, but generated an error in some cases.
- Issue 18276431: An access control may define a conflict across two roles (or responsibilities). If the control's enforcement type were Approval Required, preventive analysis would suspend the assignment of both roles. In the Manage Access Approvals page, a result investigator may then approve one role assignment and reject the other. If so, the Preview option displays the control that generated the conflict. When the investigator selects the control, the Preview display should show no result, because with one role rejected, there is no longer a conflict. Instead, it showed both roles.
- Issue 17577435: A Submit button in the Manage Access Approvals page should enable users to approve assignments, but generated an error in certain cases (Oracle EBS users with more than 60 responsibilities).
- Issue 17776251: When the GRC log threshold was set to a level other than Debug, an attempt to approve role assignments in the Manage Access Approvals page generated an error.
- Issue 17411412: Once rejected, a responsibility could not be reassigned and approved via AACG preventive analysis.

- Issue 17398281: The Manage Access Approvals page correctly displayed records of Oracle EBS responsibility assignments that violated controls whose enforcement type was Approval Required. However, it continued to display records for these assignments after the enforcement type was changed to Monitor and control analysis was performed again (an end-date extension was requested in EBS).

Synchronization Issues

Data synchronization is a process that copies data from a datasource (business application) into GRC for analysis by models and controls. Distinct processes synchronize transaction and access data. GRC 8.6.5.1000 resolves the following issues, which apply to synchronization for both AACG and ETCG:

- Issue 18289958: An attempt to synchronize transaction data resulted in an error.
- Issue 18230620: After an access synchronization job ran, analysis of an access control stalled at 50 percent completion and generated an error, even though the control ran successfully before the synchronization job ran.
- Issue 17981429: For ETCG, synchronization updates business objects used in models or controls configured to analyze risk in a selected datasource. An attempt to synchronize data for a Purchasing Approval Assignments business object (of an Oracle E-Business Suite 12.1.3 datasource) generated an error.
- Issue 17838112: An attempt to run transaction synchronization for a Cross Validation Rules business object generated an error.
- Issue 17776294: At attempt to run transaction synchronization against particular seeded models stalled at approximately two-thirds of completion.
- Issue 17669913: Problems with synchronization occurred if two jobs for a given model or control ran concurrently, and a synchronization job were then added to the queue.
- Issue 17562507: When transaction business objects were synchronized, the relationships between them were not (unless the objects were used together in a single model before synchronization was run).
- Issue 17556982: Transaction synchronization jobs, when run from the Manage Application Datasources page, failed for the MTL_CATEGORY_SETS_B table.
- Issue 17556381: Access and transaction synchronization can be initiated through web services, as an alternative to standard procedures involving the GRC user interface.
- Issue 17463826: Translation synchronization against a model that called the Journal Entry General Ledger Accounts business object took excessive time and generated an unexpectedly large number of records.
- Issue 17445395: An attempt to run transaction synchronization resulted in an ORA-00904 error.
- Issue 17431539: If a “Graph Synchronization Date Limit” is set, the synchronization of certain transaction business objects, in which records are created or updated frequently, applies only to records created or updated on or after a

specified date. The use of this feature with the Receivables Invoice business object improperly prevented some records from being selected by model filters.

- Issue 17423917: Transaction synchronization did not run successfully against models with which perspective values were associated. (A perspective is a set of related values; individual values may be associated with individual objects, such as models, controls, or incidents.)
- Issue 17285714: Access synchronization runs took excessive time to complete.
- Issue 17278059: Transaction synchronization did not work when run against transaction models that contained filters specifying custom attributes.
- Issue 17251404: An attempt to run access synchronization generated an ORA-01400 error when the job reached 62 percent completion.
- Issue 17039825: Attempts to cancel scheduled jobs to run access or transaction synchronization generated errors.
- Issue 16743779: During access synchronization runs, GRC created an excessively large number of archive files.

EGRCM Issues

EGRCM 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. Users may also assess objects, complete surveys about them, raise issues when defects are uncovered, and resolve issues. GRC 8.6.5.1000 resolves the following EGRCM-related issues:

- Issue 17637492: A worklist (notification) for an EGRCM survey remained active, and a user could open the survey, even after another user completed it and an assessment that contained it, and an assessment manager closed the assessment.
- Issue 17570472: In EGRCM, when a user created a process, related a risk to it, and submitted the process, it could not then be edited. When the process was selected in the Manage Processes page, the Edit option was inactive.
- Issue 17209279: An attempt to select the Analysis tab of the EGRCM Manage Risk page generated an error.
- Issue 16930134: When a user attempted to edit an imported risk in EGRCM, its Analysis Model field did not accept input.

Security

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 data role may also be linked to perspective values; if so, it grants access only to data concerning objects associated with the same values. GRC 8.6.5.1000 resolves the following security issues:

- Issue 17821670: Users were assigned a job role that used perspectives to provide write access to incidents generated by one control, but view access to inci-

dents generated by another control. Those users were inappropriately able to edit incidents generated by either control.

- Issue 17550489: Users without proper permissions were able to review role assignments awaiting approval in the Manage Access Approvals page.
- Issue 17449792: GRC generated worklists providing a user with privileges to review incidents generated by a CCM continuous control, although the control was associated with a perspective value that was not associated with a GRC data role assigned to the user. (This occurred because no perspective value was selected for incidents generated by the control, and so incidents were available to all users.)
- Issue 17019691: From a Manage Jobs page, users with appropriate permissions should be able to purge jobs (remove records of completed jobs). Users without appropriate permissions were also able to purge jobs.
- Issue 17019585: Users were able to run and view the Entitlement Report even if their roles did not grant them permission to do so. (The Entitlement Report lists access points belonging to each in a selection of AACG entitlements.)
- Issue 16948961: In the CCM Manage Results page, a user could see records of controls and incidents in all datasources, even though his roles should have provided access to data from one datasource.
- Issue 16556598: When assigned a duty role that should have provided view-only access to jobs, users could inappropriately cancel and purge jobs.

GRC System Issues

A job is a request to synchronize data, evaluate models or continuous controls, generate reports, or perform other background tasks. GRC assigns each job a number, which appears in a record of the job displayed in a Manage Jobs page. In earlier versions, job numbers were assigned erratically; in version 8.6.5.1000, they are generated sequentially. In addition, release 8.6.5.1000 resolves the following issues, which concern GRC generally:

- Issue 17854206: After an upgrade to GRC 8.6.4.8000 (build 8322), an attempt by Oracle Identity Manager (OIM) to make a call to the GRC database resulted in an error.
- Issue 17842076: An attempt to restart the GRC application server resulted in a WorklistSyncService error.
- Issue 17751090: To prevent “malformed UTF-8” errors, set the GRC database to use the AL32UTF8 character set, and run a “–Dfile.encoding=URF-8” JVM argument against GRC itself. (See the *GRC Installation Guide*.)
- Issue 17664457: An error occurred when nineteen users logged on to GRC and all attempted to access a single ETCG control.
- Issue 17643486: In a variety of load tests — scenarios in which varying numbers of users attempted to access a set of controls in varying timeframes — GRC generated errors.

- Issue 17636485 and 17605089: A GRC instance that connects to a Microsoft SQL Server datasource, runs with WebLogic, and implements Secure Sockets Layer (SSL) must use the Microsoft JDBC Driver 4.0 for SQL Server. See the "Special Cases Involving SQL Server" section in the "Additional Advance Controls Configuration" chapter of the *GRC Installation Guide*.
- Issue 17516678: After an upgrade from GRC 8.6.4.3347 to 8.6.4.4240, the log-on page was unavailable and the log recorded an error.
- Issue 17490121: Entries users can select in LOVs are stored as "lookups," which are configurable. Each lookup includes a lookup code, which must consist of 30 or fewer characters. Validation has been added to ensure that codes do not exceed the maximum length as they are created.
- Issue 17419630: An attempt to upgrade to GRC 8.6.4.8000 (build 8322) failed. This was related to two clusters being open during application initialization.
- Issue 16892250: Custom and JDBC connectors were updated for DB2 support.
- Issue 16862644: Uses can define search criteria for lists of objects on GRC management and overview pages, and should be able to save and select searches. In the Manage Jobs page, however, saved searches did not appear in the list box from which they should be selected.
- Issue 16718896: After WebLogic middleware components were upgraded, an attempt to run GRC in Windows Internet Explorer 9 generated compatibility errors. GRC 8.6.5.1000 uses a later version of middleware components than those involved in this error. IE9 remains one of the web browsers that can display GRC.
- Issue 16622883: GRC performance declined when the GRC database was configured to use Real Application Clusters (RAC).

GRC Reports

Apart from GRCI, GRC offers a selection of reports that may be run from a Report Management page or (in some cases) "contextually" — in the CCM pages in which controls are created or incidents are reviewed. GRC 8.6.5.1000 resolves the following issues, which concern these reports:

- Issue 18191440: In AACG, a condition specifies users or other objects that are excluded from SOD analysis. A Conditions Report provides information about three types of condition: global, path, and control-specific. The report did not list values for sets of books, MO: operating units, data groups, and AK region codes that were excluded by global conditions.
- Issue 17852546: When a single datasource was selected as a parameter for the Global Users Report, the report showed information about all datasources. (Global users are IDs created for AACG. Each identifies one person, but correlates to any number of potentially varying IDs that person may have in business applications subject to access controls.)
- Issue 17790218: A Transaction Incident Details Report failed if run for a control whose incident data included non-ASCII characters.
- Issue 17576646: Attempts to run any CCM report generated an error.

- Issue 17556406: The Access Violations Within a Single Role (Intra-Role) Report and Intra-Role Violations by Control Report did not show any violations, although intra-role violations were known to exist.
- Issue 17515257: Comments written for incidents in Result Management were not included in the Result Summary Extract Report or Access Incident Details Extract Report.
- Issue 17464930: When the Access Violations by User Report was run with a control and datasource selected as parameters, differing numbers of incidents were returned for users assigned the same role.
- Issue 17457184: A typical first step in the running of a contextual report is to filter the list of controls or incidents to include only those for which the report should display information. GRC inappropriately limited report content further to records of controls or incidents that were highlighted in their grids.
- Issue 17457116: When the Transaction Incident Details Extract Report was run from the Manage Results page, there were discrepancies between report content and incident data displayed in the Manage Results page.
- Issue 17387470: The Access Violations Within a Single Role (Intra-Role) Report returned results only if one or more controls were specified as parameters as the report was run. (It should be able to return results for all controls to which a user has access if no control is specified.)
- Issue 17172046: After an upgrade, an attempt to view the Access Incident Details Extract Report generated an error.
- Issue 17043273: An attempt to run the Access Violation by User Report, with four controls selected as a parameter, generates an error. (When the report is run with each control selected individually, only one of the controls precipitates an error.)
- Issue 16980475: The Access Violations by User Report returned incorrect results when run against multiple controls.
- Issue 14021925: A Pending Activities Report was enhanced so that access to it could be secured through the use of perspective values associated with data roles.

GRCI and the DA Schema

Each GRCI dashboard displays a set of reports that provide broad graphic and tabular views of data. From each report, users can “drill down” to other reports that provide more detailed and focused views. GRCI displays data from a Data Analytics (DA) schema, which is separate from, but updated by, the main GRC database schema. GRC 8.6.5.1000 resolves the following issues, which concern GRCI and the DA schema:

- Issue 18106679: GRCI dashboards include lists of values from which users may select parameters that narrow the focus of reports. A date parameter LOV did not include the year 2014.

- Issue 17910881: DA schema updates are scheduled in an Analytics tab of a Manage Application Configurations page. However, an attempt to schedule an update generated an error.
- Issue 17785800: A GRCI dashboard failed to maintain relationships among AACG controls, the incidents they generated, perspectives, and entitlements.
- Issue 17582634: The DA schema can be updated through web services, as an alternative to the standard procedure involving the GRC user interface.
- Issue 17556566: Enhancements to DA schema updates improve performance.
- Issue 17537230: A DA schema update required excessive time.
- Issue 17307724: A job to refresh the DA schema did not update the GRI_D_CONTROL_B and GRI_D_CONTROL_TL tables.
- Issue 17290038: An attempt to drill down from the Open Issues by Severity report to a view of EGRCM controls tested in a specified assessment resulted instead in a view of all EGRCM controls.
- Issue 17243501: After a job to refresh the DA schema, GRCI dashboards did not display expected data for some objects.
- Issue 17220854: A GRCI report displayed incorrect counts for CCM incidents at the Closed status.
- Issue 17206839: A GRCI report displayed incorrect results for run and update dates associated with CCM controls and incidents.
- Issue 17000848: An attempt to open the GRCI Certifications dashboard, which provides reports about EGRCM assessments, generated an error.
- Issue 16881646: In the DA schema, AACG entitlement data was not stored with incidents. Thus a custom GRCI report combining entitlement name, incident count, user count, and role count could not be created.
- Issue 16810567: Users may create user-defined attributes (UDA) for EGRCM controls, risks, processes, or other objects — information that extends the definition of an object. A UDA field may allow users to select from among a set of values, and if so, those values are stored as a "lookup." Each lookup value consists of a code and a meaning, and GRCI reports incorrectly displayed the code rather than the meaning.
- Issue 16810212: After a refresh of the DA schema, some UDAs were not updated in GRCI reports.
- Issue 16694189: GRCI reports did not display values for EGRCM remediation plans and tasks.

Translation

GRC may display data in up to twelve languages. An administrator uses the Manage Application Configurations page to make a selection of these languages available to users. GRC 8.6.5.1000 resolves the following translation issues:

- Issue 17979621: An attempt to display incident (control-violation) data for several seeded controls in French generated an error.

- Issue 17886039: When a user logged on to GRC in French, AACG entitlement data remained in English.
- Issue 17853207: When a user logged on to AACG in French, incidents were not displayed correctly for French.
- Issue 17518327: New seeded content (Oracle-created CCM models) is available for GRC 8.6.5.1000, and that content is translated.
- Issue 16762489: When a user created a UDA in one language, logged on in another language, and translated the UDA display label into that language, the change persisted when users once again logged on in the first language.
- Issue 16563787: An EGRCM module created in one language could be viewed (with appropriate translations) in another language, but an attempt to edit the module in that second language caused GRC to freeze.

Known Issues

The following issues are known to exist in version 8.6.5.1000 of GRC, and will be addressed in future releases.

- Issue 18269870: In AACG, when models generate results or controls generate incidents, a visualization feature can display graphical depictions of the access points involved in conflicts. Currently, a complete path from user to privilege is difficult to follow.
- Issue 18262995: In AACG, a user-defined access point (UDAP) is a specific path to a seeded access point. It may be used in a model or control as if it were an access point. A UDAP is defined in the page in which entitlements are created, and two columns intended originally for use with entitlements — Access Control and Change Control Audit — remain inappropriately available to users as they create UDAPs.
- Issue 18246717: AACG controls may be assigned any of three enforcement types, one of which is Monitor. When a business-application user is assigned roles that violate a Monitor control, AACG preventive analysis should (and does) allow the assignment. If the control is subsequently run, however, the assignment should generate incidents at the Assigned status (meaning that a result investigator should look into them). Instead, it generates incidents at the Approved status. (This status is appropriate only when the assignment of roles triggers a control whose enforcement type is Approval Required, approval is granted in the Manage Access Approvals page, and the control is subsequently rerun.)
- Issue 18232728: In AACG, a path condition defines a path from a parent access point to a child access point, and excludes it from analysis. A Manage Access Path Conditions page lists the path conditions configured for an AACG instance. In it, a Date Changed column should show the date on which each path condition was last edited, but shows the system date instead.
- Issue 18224108: When dates are entered as parameters for the Access Incident Details Extract Report, the report displays date parameter values as blank.

- Issue 18223859: If a user filters the models listed in the Manage Access Models page, then uses any of the Copy, Delete, or Export options, the page refreshes and displays the full, rather than filtered, list of models.
- Issue 18220336: When a user attempts to import a CCM model file while another model-import job is running, GRC cancels the second attempt, rather than add it to the jobs queue.
- Issue 18175993: In EGRCM, an issue is a defect or deficiency detected for an object or for an activity being performed against an object, and a remediation plan is a set of tasks that, when completed, will resolve an issue. When a user selects a Mark Complete option while working with a remediation plan, the status of the plan remains Active rather than Completed.
- Issue 18103280: In AACG, simulation previews how resolutions of access incidents would affect the business application in which those incidents exist. It consists of "remediation steps," each of which hypothetically breaks the connection of an access point to a parent access point, and so resolves an incident. When a users saves a simulation and then runs it, one or more remediation steps disappear.
- Issue 17967262: In the Manage Results page, a user may create a list of incidents generated by a single control, then use search features to refine that list further. The user may select basic or advanced search; the latter (in part) offers more fields on which to search, and permits the user to add fields to those provided by default. If the user is searching among incidents generated by a transaction control, the fields available to be added to a search are appropriate to an access control.

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.

Installation and Upgrade

You can install GRC 8.6.5.1000 independently of past releases, or you can upgrade to it from version 8.6.4.7000, 8.6.4.8500, or 8.6.4.8900.

If you upgrade, you will need not only to upgrade GRC itself, but also to install new versions of the middleware components that support it. Also, 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”).

Be sure to back up data for your earlier instance before you upgrade to 8.6.5.1000.

If you expect to install GRCI but may postpone doing so until a later upgrade, create a DA schema as you install GRC 8.6.5.1000. You can install GRCI with a later, upgrade-only release of GRC only if you create the DA schema now. (This applies regardless of whether you are performing a new installation of GRC 8.6.5.1000, or are upgrading from an earlier version in which you had not set up GRCI.)

As you install GRC 8.6.5.1000, 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: `8406a5f28e422cec1405125fd4058d41`
- grc.war: `f9d9471061e1bf808e075724a80f2f30`

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