

Governance, Risk, and Compliance Controls Suite

Release Notes

Software Version 7.2.2.1

ORACLE®

Governance, Risk, and Compliance Controls Suite Release Notes

Part No. AG008-7221A

Copyright © 2007, 2008, Oracle Corporation and/or its affiliates. All rights reserved.

The Programs (which include both the software and the documentation) contain proprietary information; they are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright, patent, and other intellectual and industrial property laws. Reverse engineering, disassembly, or decompilation of the Programs, except to the extent required to obtain interoperability with other independently created software or as specified by law, is prohibited.

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. This document is not warranted to be error-free. Except as may be expressly permitted in your license agreement for these Programs, no part of these Programs may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose.

If the Programs are delivered to the United States Government or anyone licensing or using the Programs on behalf of the United States 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, use, duplication, disclosure, modification, and adaptation of the Programs, including documentation and technical data, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement, and, to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software — Restricted Rights (June 1987). Oracle Corporation, 500 Oracle Parkway, Redwood City, CA 94065.

The Programs are not intended for use in any nuclear, aviation, mass transit, medical or other inherently dangerous applications. It shall be the licensee’s responsibility to take all appropriate fail-safe, backup, redundancy and other measures to ensure the safe use of such applications if the Programs are used for such purposes, and we disclaim liability for any damages caused by such use of the Programs.

The Programs may provide links to Web sites and access to content, products, and services from third parties. Oracle is not responsible for the availability of, or any content provided on, third-party Web sites. You bear all risks associated with the use of such content. If you choose to purchase any products or services from a third party, the relationship is directly between you and the third party. Oracle is not responsible for: (a) the quality of third-party products or services; or (b) fulfilling any of the terms of the agreement with the third party, including delivery of products or services and warranty obligations related to purchased products or services. Oracle is not responsible for any loss or damage of any sort that you may incur from dealing with any third party.

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

The license for this program includes a limited use license for the Internal Control Manager program. Such limited use license means that the Internal Controls program shall only be used for financial compliance or IT governance related operations.

Contents

GRC Controls Suite 7.2.2.1 Release Notes..... 1

 Oracle Applications Release 12.....2

 Data Access Sets.....3

 AZN Menu Exclusions 4

 RBAC 4

 Auditing.....4

 SOD Content.....7

 Other Access Provisioning Issues 7

 Reports.....9

GRC Controls Suite 7.2.2.1 Release Notes

In version 7.2.2.1, LogicalApps ACTIVE Governance is rebranded as an Oracle product — Governance, Risk, and Compliance Controls Suite. The product continues to document and enforce business controls, enabling users to demonstrate regulatory compliance and to promote operational efficiency.

- In earlier versions, an ACTIVE Governance Platform documented a “control Library,” enabling users to define not only controls, but also other objects whose hierarchical relationships to one another form a “control framework.” In version 7.2.2.1, the platform continues to serve these purposes, but is no longer considered a distinct product. Instead, it is a platform in which GRC Controls Suite products run.
- ACTIVE Access Governor has become, in version 7.2.2.1, Application Access Controls Governor. It continues to uncover segregation-of-duties (SOD) conflicts within an organization, and to audit users’ users temporary access to duties they do not ordinarily fulfill.
- ACTIVE Policy Governor has become, in version 7.2.2.1, Transaction Controls Governor. It implements “control monitors,” each of which uses structured query language (SQL) statements to select records of actions subject to control and marks them as “suspect tasks.”
- ACTIVE Data Governor, as well as elements formerly known as Embedded Agents, has become Preventive Controls Governor. Its Change Control Wizard implements change-control rules within instances of Oracle E-Business Suite;

Form Rules modifies the security, navigation, field, and data properties of Oracle forms; Flow Rules executes business processes; and Audit Rules audits database tables.

In addition to these rebranding changes, Oracle Governance, Risk, and Compliance Controls Suite runs with Oracle E-Business Suite Release 12 (as well as with releases that were supported by, or preferred for, version 7.2.1 of ACTIVE Governance). The *Product Support Matrix* lists all supported and preferred Oracle releases.

Version 7.2.2 also introduces two new reports and addresses other reporting issues, resolves issues with its auditing functionality, enhances its “SOD content” (a set of SOD rules that may be customized for site-specific use), and effects other improvements in access provisioning.

Version 7.2.2 incorporates the following hotfixes: 721AAX06.1 (which includes 721AAX01, 721AAX03, 721AAX04, and 721AAX05), 721AAX02, 721RC01, and 721AR02.1.

Oracle Applications Release 12

GRC Controls Suite version 7.2.2 works with Oracle Applications Release 12, with limitations. First, in Release 12, some E-Business Suite forms are replaced with HTML pages designed according to the OA Framework. Rules written in the Form Rules application do not work with OA Framework-based pages. They do work with older-style forms that remain in Oracle Release 12, and they work without limit in versions of Oracle Applications earlier than Release 12. Other Embedded Agents work without limitation in both Release 12 and earlier versions of Oracle Applications.

Application Access Controls Governor enables users to create SOD rules, each of which specifies two or more responsibilities or functions that should not be assigned simultaneously to an individual person. Each rule applies a “control type” that determines the action to be taken when an Oracle Applications user is assigned duties that violate the rule. Two of these are Allow with Rules and Approve with Rules; for each of these, an associated form rule alters an Oracle form to mitigate the conflict defined by the SOD rule.

In version 7.2.2.1, these rules continue to work correctly when they target responsibilities or functions accessible from older-style forms. However, when SOD rules with the Allow with Rules or Approve with Rules control type define conflicts in functions or responsibilities accessed through OA Framework-based pages, they do not produce desired results — they detect conflicts, but the implication that those conflicts are mitigated by form rules is incorrect, because form rules do not work on such pages. For such SOD rules, the control type should be changed to either of the other two options, Prevent or Approval Required.

Second, the Access Monitoring feature does not work when Application Access Controls Governor is connected to a data source that runs Oracle Release 12. It continues to work correctly when Application Access Controls Governor is connected to a data source running an earlier version of Oracle Applications.

Data Access Sets

In Oracle EBS, a data access set is a collection of ledgers or ledger sets (a ledger set itself being a collection of ledgers) that can be accessed by a responsibility. The data access set can grant read/write or read-only access to each member of the set — each ledger, balancing segment value, or management segment value. Through the use of a profile option called GL: Data Access Set, a system administrator associates each data access set with a responsibility. Each responsibility can have only one data access set assigned, but each data access set can be assigned to more than one responsibility.

A user creating an SOD rule in Application Access Controls Governor has in the past been able to set Same Operating Unit and Same Set of Books options. These options remain in version 7.2.2.1, providing that Access Governor is connected to a data source that runs Oracle Applications 11.5.3–11.5.10. When Access Governor is connected to an Oracle Release 12 instance, the Same Operating Unit option remains, but the Same Set of Books option is replaced by three options that accommodate ledgers and data access sets — Same Ledgers, Same Access Sets, and Ignore Read Only. (These options appear as check boxes on the Add, View, Edit, and Copy SOD Rule panels.)

Appropriate settings for these options are as follows:

- **Same Operating Unit:** Select the check box to have the rule generate a conflict only if a user's responsibility assignments would grant access to base and conflicting "entities" (responsibilities or functions) within an individual operating unit. Clear it to have the rule apply across operating units as well.
- **Same Set of Books:** Select the check box to have the rule apply only if a user would have access to base and conflicting entities within an individual set of books. Clear it to have the rule apply across sets of books as well.
- **Same Ledgers:** Select the check box to have the rule generate a conflict only if the conflicting entities would enable a user to access data in an individual ledger (because the ledger is included in data access sets assigned to responsibilities involved in the conflict). Clear the check box to have the rule generate conflicts across ledgers.
- **Same Access Sets:** Select the check box to have the rule generate a conflict only if the conflicting entities would enable a user to access data in ledgers belonging to a single data access set (because that access set is assigned to responsibilities involved in the conflict). Clear the check box to have the rule generate conflicts across data access sets.
- **Ignore Read Only:** Select the check box to have the rule generate a conflict if the conflicting entities would grant write access to ledger data, but not when either entity would grant read-only access (because data access sets are configured to grant read-only access). Clear the check box to have the rule generate conflicts regardless of whether ledger-data access is read-only or write.

Oracle automatically generates a "system" data access set for each ledger or ledger set that is created. These provide write access at the full-ledger level. So if you use system data access sets, the Ignore Read Only option has no meaning.

In Application Access Controls Governor, a Simulation feature enables users to write rules, each of which names a function or menu that might be excluded from a responsibility, or a function or submenu that might be removed from, or inserted in, a menu. As it evaluates these rules, Application Access Controls Governor determines how conflict generation would differ if the simulated conditions were in force. In version 7.2.2.1, the Simulation feature has been updated to evaluate the Same Ledgers, Same Access Sets, and Ignore Read Only settings correctly. However, this does not impose any change in the way a user would use the Simulation feature.

AZN Menu Exclusions

In Release 12, Oracle EBS introduced the ability to configure exclusions for AZN menus. The Application Access Controls Governor SOD engine is updated to recognize AZN menu exclusions (to treat them as it would other exclusions).

RBAC

Oracle EBS users may be directly assigned responsibilities, each of which provides access to a menu, which in turn provides access to other menus, functions, or both. Or, through a feature called Role Base Access Control (RBAC), users may be assigned roles, either in addition to or instead of responsibilities. Each role comprises any combination of responsibilities, other roles, functions (also called permissions), and data-security policies.

Application Access Controls Governor SOD rules set responsibilities in conflict with other responsibilities, or functions in conflict with other functions. The application detects rule-defined conflicts between the responsibilities assigned to each user or between functions to which those responsibilities give access.

If you create roles in Oracle and assign them to users, Application Access Controls Governor performs conflict analysis correctly if the roles contain only responsibilities. If roles contain functions or data-security policies, Application Access Controls Governor performs conflict analysis correctly for responsibilities assigned to roles and the functions to which those responsibilities give access, but not for the functions or data-security policies assigned to the roles independently of responsibilities.

Thus, to maintain the integrity of Application Access Controls Governor SOD analysis, configure each role in Oracle Applications so that it contains only responsibilities.

Auditing

Version 7.2.2.1 of GRC Controls Suite corrects auditing problems, not only in the Audit Rules application, but also in the applications to which it provides functionality — Preventive Controls Governor and the Access Monitoring feature of Application Access Controls Governor. Many of these problems concern audit translations, which are meaningful values — either entries held in lookup tables or constants — that correspond to values held in audited tables. For example, a person's actual name

might be the translation value when an audited table column holds a numeric ID for the person.

Issues AGM-847 and AGM-852

To perform auditing, the Audit Rules application establishes database triggers in database tables used by Oracle EBS. In such a database, there may be multiple schemas, and instances of a given table may exist in more than one schema. For such tables, Audit Rules could not create triggers properly, because it expected tables to be unique. In version 7.2.2.1, Audit Rules can establish triggers correctly even for a table with instances in multiple schemas.

Issue AGM-875

Users select tables for auditing by assigning them to groups, and refine audits further by selecting columns from the tables that belong to each group. An Update Audit Objects program is then run to implement auditing on the defined groups. In earlier versions, the Update Audit Objects program could set incorrect primary keys for certain tables. Version 7.2.2.1 corrects this error.

Issue AGM-848

When, through Access Monitoring, a user receives temporary access to responsibilities or database tables, her actions are audited. Records of these actions are stored in the `laud_audit_transactions` database table, which supplies data to the Access Monitoring User Activity Report. When those actions involved changes to more than one database table, data from those tables was misaligned as it was stored in `laud_audit_transactions`, and so the Access Monitoring User Activity Report displayed incorrect data. Version 7.2.2.1 corrects the insertion of data into the `laud_audit_transactions` table, so that the Access Monitoring User Activity Report presents audit data correctly.

Issue AGM-854

A concurrent request called Audit: Dequeue Process compiles audit data so that reports for the Audit Rules and other audit-dependent applications can display current data. In earlier versions, when changes had been made to multiple database tables, data from varying tables was misaligned as it was compiled. Version 7.2.2.1 corrects the misalignment so that audit data is reported correctly.

Issue AGM-860

When a change is made to an audited database column, Audit Rules stores old and new values in the `laud_audit_transactions` table, for later inclusion in reports. If a translation were created for such a column, Audit Rules should have stored the old and new translated values in `laud_audit_transactions`. Owing to a fault in the audit engine, it instead stored the translation for the new value in place of both the new and old actual values. If, for example, the value in an ID column changed from 111 to 222, and the proper translation for 111 were Peter and for 222 were John, the application stored both the old and new values as John. Version 7.2.2.1 corrects this error.

Issue AGM-858

In earlier versions, an existing translation could not be modified. Although a user could edit or delete a translation in Audit Rules, and the application would appear to save the change, in fact the modification would not take effect. The original translation would still apply. In version 7.2.2.1, when a translation is edited the new translation takes effect, and when a translation is deleted, the application reports actual audited values rather than translated values.

Issue AGM-870

In place of values from a lookup table, one can designate a constant value as an audit translation. However, a necessary identifier was not being generated for inclusion in the table in which the constant value would be stored, and so insertions in this table would fail; as a result, such translations would not work. Version 7.2.2.1 corrects this error, and constant-value translations work correctly.

Issue AGM-853

One may upload “seeded content” — a set of change-control rules — for Preventive Controls Governor. In part, change control involves auditing changes to form fields, and to carry out its auditing requirements, the Change Control component of Preventive Controls Governor uses Audit Rules. Every form field corresponds to a database column; for each form field subject to a change-control rule, the Audit Rules application monitors the corresponding database column.

In earlier versions, the audit engine required that constant values used for translations be enclosed in single quotation marks. Thus, when a seeded change-control rule included a translation that incorporated a constant value, that value was provided in single quotation marks.

In version 7.2.0, the audit engine was redesigned to remove certain dependencies. One effect of the change was that single quotation marks were no longer permitted around constant values used in translations, and so seeded rules including such translations failed. In version 7.2.2.1, the audit engine is modified so that it once again requires single quotation marks around constants used in translations. Thus seeded change-control rules including such translations once again work properly.

Issue AGM-859

For auditing in support of Access Monitoring, translations for primary-key values would not work. Instead of displaying the translation configured for a primary key, the Access Monitoring User Activity Report would display the actual primary-key value. Version 7.2.2.1 corrects this error.

Issue AGM-861

When a translation configured for a primary-key value involved a lookup value whose column type was other than NUMBER, the translation did not work. Version 7.2.2.1 corrects this error.

Issues AGM-863 and AGM-876

The Change History Report displays the old and new values for changes made to fields that are subject to change control. For fields corresponding to columns for which translations were configured, the old and new values displayed in the report were not translated. Version 7.2.2.1 corrects this error.

Issue AGM-865

Audit reports can be run in either of two environments, one of which is a reports browser in the GRC Controls Suite platform. This report is divided into sections corresponding to tables within audit groups; the header of each section identifies the primary keys for the table. In earlier versions, records of audited changes would sometimes appear under the wrong primary key. Version 7.2.2.1 corrects this error.

Issue AGM-866

When displaying audit results for columns for which translations were configured, the audit report that runs in the GRC Controls Suite platform reports browser should show the translations for the old and new values. In earlier versions it did not. Version 7.2.2.1 corrects this error.

Issue AGM-801

Audit reports can also be defined and run in the Oracle EBS environment. This report was failing to display audit data, instead presenting the message “no data found.” Version 7.2.2.1 corrects this problem, so that the EBS-environment audit report displays audit data properly.

SOD Content

An “SOD content spreadsheet” contains SOD rules that users can edit to meet their needs, and then upload into Application Access Controls Governor all at once. Version 7.2.2.1 resolves the following content issues.

Issue AGS-1659 and AGM-759

For a function-based SOD rule, the conflicting functions may, but need not, be associated with applications. In earlier versions, the content-loader program was unable to upload a set of rules if it included a rule in which a function was not associated with an application. Version 7.2.2.1 corrects this problem, and the content-loader program uploads rules regardless of whether functions are associated with applications.

Issues AGS-1650 and AGM-802

An SOD rule may be associated with a form rule, allowing (or requiring approval for) access if the form rule alters an Oracle form in a way that mitigates the conflict defined by the SOD rule. Moreover, an SOD rule may designate an approval group that reviews conflicts generated by the rule. The content-loader program was failing because it did not accommodate form rules or approval groups. Version 7.2.2.1 updates the content loader to handle values passed in for these components, and the content spreadsheet has been altered to include columns in which users can enter the values.

Other Access Provisioning Issues

GRC Controls Suite version 7.2.2.1 also includes the following improvements to access provisioning:

Issue AGM-891

An “intraresponsibility” conflict is one that involves only one responsibility, because functions available from it are set in conflict or because the responsibility is set in conflict with itself. When the assignment of a responsibility to a user generates two or more intraresponsibility conflicts, the rejection of any one of these conflicts should prevent the user from accessing the responsibility, even if the other conflicts are approved. In earlier versions, however, access was denied only if all such conflicts were rejected. Version 7.2.2.1 corrects this error, so that the rejection of any one in a set of intraresponsibility conflicts properly denies access to the responsibility.

Issue AGM-895

An “interresponsibility” conflict is one that involves two responsibilities, either because two functions are defined as conflicting and each is available from a distinct responsibility, or because two responsibilities are set in conflict. When the assignment of a responsibility to a user generates two or more such conflicts, and they involve a second responsibility to which the user already has access, the rejection of any one of these conflicts should prevent the user from accessing the new responsibility, even if the other conflicts are approved. In earlier versions, however, access was granted. Version 7.2.2.1 corrects this error, so that the rejection of any one in a set of interresponsibility conflicts properly denies access to the newly assigned responsibility.

Issue AGM-881

Within Application Access Controls Governor, a Generate User Conflicts program determines whether assignments of responsibilities to users violate SOD rules. Under certain circumstances — the existence of a very large number of active SOD rules, or the creation of Oracle menus in which functions are embedded as many as ten levels deep — the Generate User Conflicts program would “hang.” Version 7.2.2.1 implements performance tuning, so that the Generate User Conflicts program no longer hangs under these conditions.

Issue AGM-636

In Application Access Controls Governor, “global subscribers” identify entities — users, submenus, functions, data groups, or operating units — that are exempt from SOD rules. One should not be able to create or modify global subscribers while the Generate User Conflicts program is running, as this would necessarily distort the results, in effect producing a set of conflicts in which some are generated to a different standard from others. In version 7.2.2.1, one cannot do so, and an error message is displayed if a user attempts to create a global subscriber while the Generate User Conflicts program is running.

Issues AGS-1661, AGS-1658, and AGM-788

Access Monitoring enables users to request temporary access to database tables or to Oracle responsibilities, for themselves or for others. When a responsibility request is approved, the user granted access receives an email message informing him of the rights he has been assigned. Along with other information, it should provide an ID and password he can use to log on to the responsibility. In earlier versions, the password was missing from these messages. Version 7.2.2.1 corrects this error.

Issue AGM-677

Within Application Access Controls Governor, a Populate User Access Data Table program updates a database table that contains information about users’ responsibility, menu, and function assignments. The table provides this information to the SOD Remediation Impact Report and the Oracle EBS Security reports when they are run.

Version 7.2.2.1 adds a parameter — Only Active Responsibilities — to this program. Select Yes to have the program return data pertaining only to users’ active responsibilities (and exclude users who have been assigned no active responsibilities). Select No to have the program return all data for users assigned any responsibilities, whether active or inactive.

Reports

The GRC Controls Suite platform provides a reports browser, in which users can view reports about the control framework configured in GRC Controls Suite, the control monitors that enforce controls, segregation of duties processing, Access Monitoring requests, change-control rules, the performance of the Embedded Agents, and other features. Version 7.2.2.1 addresses the following reporting issues.

Issues AGS-1615, AGS-1149, AGM-639, and AGM-731

Version 7.2.2.1 adds two new reports, both of which are available in the Access Monitoring folder of the reports browser.

- The Access Monitor Request Report lists requests for database or responsibility access generated through use of the Access Monitoring feature. Each listing identifies the requested responsibility or database table, the user for whom access is requested, and the approver; the ID of the request and its status (as well as the support ticket with which it is associated, if any); and the dates on which access was requested, would start, and would end.
- The Access Requests Awaiting Approval Report lists pending conflicts uncovered through “preventive” SOD analysis.

Preventive analysis is the automatic distribution of approval messages within Oracle when SOD rules are triggered by the creation of a new user or the assignment of new responsibilities to an existing user. It’s implemented by a form rule, but that rule can be disabled. (In that case, Application Access Controls Governor would perform only “detective” analysis — it would identify conflicts, but do nothing in Oracle Applications to resolve them.) If preventive analysis is disabled, then re-enabled, the Access Requests Awaiting Approval Report lists pending conflicts generated after preventive analysis is re-enabled. A pending conflict is one for which the SOD rule owner (or approval group) has received an approval message in Oracle, but has not yet made an approval decision.

GRC Controls Suite users are assigned roles, which determine the features they can use. Only a user at the AG Super User role is able to open or run these two reports.

Issue AGS-1628

A User Conflicts Trend Analysis Report charts changes in the number of outstanding user conflicts over time. The word *outstanding* indicates those that have not been resolved, with new conflicts added in and those that have been resolved subtracted out. To capture a span of time, a user should be able to select, as parameters to the report, any number of “snapshots” — occasions on which user conflicts have been generated. In earlier versions, only one snapshot could be selected. Version 7.2.2.1 corrects this problem, enabling the user to select multiple snapshots.

Issue AGS-1632

The reports browser lists not only the titles of reports available for selection, but also descriptions of the reports. For version 7.2.2, these descriptions have been edited for clarity and brevity.

