Oracle® Enterprise Governance, Risk and Compliance Controls

Functional Upgrade Guide

Release 8.6.4.3000

Part No. E36200-02

April 2013

ORACLE

Oracle Enterprise Governance, Risk and Compliance Controls Functional Upgrade Guide

Part No. E36200-02

Primary Author: Stephanie McLaughlin

Contents

EGRCC Functional Upgrade

EGRCC Functional Upgrade

Oracle Governance, Risk and Compliance consists of several applications, which, in the past, have run separately from one another:

- 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.
- Enterprise Governance, Risk and Compliance Controls (EGRCC) enables users to create models and controls and to run them within business applications to uncover and resolve segregation of duties violations and transaction risk.
- Fusion GRC Intelligence (GRCI) provides dashboards and reports that present summary and detailed views of data generated in EGRCM and EGRCC.

In version 8.6.4.3000, Oracle takes significant steps toward merging these applications to produce a consolidated GRC offering that leverages their strengths. In the consolidated offering, the term "Continuous Control Monitoring," or "CCM," applies to all the functionality offered by EGRCC.

If you use an earlier version of EGRCC as a stand-alone application, you can upgrade to version 8.6.4.3000 of EGRCC (CCM) and continue to use it as a stand-alone application. Even if you do, however, it incorporates significant changes that serve to unify it with EGRCM. New features include:

- Perspectives — sets of related values. Users can associate individual perspective values with individual objects (such as models and controls), thus cataloging objects by organization, region, or any other concept a company determines to be meaningful.

  Earlier EGRCC versions enabled users to create tags, which were quite similar. However, perspectives are more powerful: First, they are hierarchical — values have parent/child relationships to one another. Second, perspectives do more than serve as filtering values in the pages in which users manage objects. They also play an important role in GRC security, and in the assignment of "incidents" generated by controls to "result investigators" (formerly "participants").

- Redesigned security, in which job roles, consisting of duty roles and data roles, provide a much more granular means of safeguarding access to GRC functionality and data.
- The use of "worklists" and "notifications" to alert users to tasks awaiting their attention. This involves modification of the system for email notification that was used in earlier EGRCC versions.
- Revised search and saved search functionality, which replaces the "views" that existed in earlier EGRCC versions.
- More robust saved report parameters.

This *Functional Upgrade Guide* is meant to give some visibility on what to expect after upgrading to version 8.6.4.3000, including examples of what an upgraded user's current access might look like with the new role-based data-level security.

Run Reports Before Upgrading

As with any patch application or upgrade, it makes good business sense to verify data integrity and functionality in a preproduction instance. Verifying data integrity requires knowing what your data is *before* you upgrade, and validating that the data remains as expected *after* the upgrade.

Before upgrading, customers may find it prudent to run several reports to be used for comparison purposes after upgrade. Because the purpose is to validate data integrity, it is probably not necessary to have reports containing all data. Rather, select a few key controls and their results, select a few users and their security access, and run reports on them. In areas where there is generally not a lot of data — such as global and path conditions — running reports that include all of the data may make sense.

Consider running and saving the following reports prior to upgrade:

- Control Detail Extract — Select a few key controls.
- Access Incident Detail Extract — Select the same key controls used in the Control Detail Extract report.
- Conditions Report — Running for all data would generally make sense.
- Access Approvals Report — Running for all data would allow validation of pending, rejected and approved access approvals.
- GRCC Users and Roles Report — Select several users with varying access.

After upgrading, run the same reports with the same parameters, and validate that data is as expected. Note: The GRCC Users and Roles Report has been replaced with the Role Assignment Report. In addition, after upgrading, run the Unassigned Perspective Values Report and the Inaccessible Records Report to be sure all records are secured properly.

Replace Participant Groups Before Upgrading

In version 8.6.3 and before, users specified as "participants" had access to controls or to the incidents they generated. A user could be assigned individually as a participant to a control, or the user (along with others) could belong to a participant group assigned to the control.

Beginning with version 8.6.4.3000, EGRCC no longer recognizes participants or participant groups. Instead, users have access to controls and (as "result investigators") to incidents if they are granted data roles associated with perspective values that match perspective values associated with the controls.

Users assigned individually as participants to controls in version 8.6.3 are mapped to the upgraded versions of those controls in version 8.6.4.3000 (and a perspective is create automatically during the upgrade for that purpose). No provision is made, however, for upgrading participant groups. Therefore, before you upgrade, identify controls to which participant groups are assigned and, for each of those controls, reassign members of the group as individual participants:

1. In the version 8.6.3 Manage Controls page, unhide the Participants column, so that the values assigned to controls are visible.
2. Select the controls to which participant groups are assigned, so that you can execute a mass update.
3. Select Actions > Assign. Remove the participant groups, and replace them with the participant users who should have access to the controls. Save your work.

Repeat these steps as necessary until all participant groups have been replaced by individual participants.

Security

In version 8.6.3 and before, EGRCC was secured through the use of roles that identified view and update access to pages and reports, as well as access to business objects and datasources. These roles were assigned to users. In addition, only the user who created a model could access it, and only "participants" assigned to controls had access to those controls or the incidents they generated.

Beginning with version 8.6.4.3000, EGRCC adopts an entirely different security model. Administrators can create "duty roles" (which specify sets of privileges) and "data roles" (which define sets of data), combine duty and data roles into "job roles," and assign job roles to users. Administrators can, therefore, define not only the work a user can do, but also the data upon which he can perform that work.

Moreover, an administrator can associate perspective values to data roles, permitting more granular data-level security. Assuming, for example, that a Region perspective includes a US value, and a Business Process perspective includes an Order to Cash value, it would be possible to create roles that permit access only to data associated with the Order to Cash process in the US region.

The new security model enables a company to be much more precise and flexible in selecting the functionality and data with which each user works.

After the upgrade to version 8.6.4.3000, users will continue to have the exact same access as they had prior to the upgrade. Existing access will automatically be mapped to new job, duty, and data roles as necessary. As noted earlier, a perspective (called "Participant Group") will automatically be created to retain the 8.6.3 participants (but not groups) for controls and incidents.

The following sections describe the methodology and naming conventions used to upgrade users, map participants to objects, create and map duty and data roles to job roles that are ultimately assigned to upgraded users.

Page Access Mapping to Job, Duty, and Data Roles

The following table shows page access in version 8.6.3, and equivalent data and duty roles in version 8.6.4.3000. After upgrade, users will continue to have the access they had prior to it. Run the GRCC Users and Roles report prior to the upgrade, and use it as a reference point.

For instance, if a Control Manager role gave a user update access to the Manage Controls page in version 8.6.3, you should expect that user to have the Manage Continuous Controls and Continuous Control Analytics duty roles, as well as the Access Control Manager and Transaction Control Manager data roles in a Control Manager job role created by the upgrade.

Page Access in 8.6.3	Duty Role in 8.6.4	Data Role in 8.6.4
Home	GRC Home Page Access	(Not applicable)
Manage Controls		
Update access	Manage Continuous Controls Continuous Control Analytics	Access Control Manager Data Role Transaction Control Manager Data Role
View access	View Continuous Controls Continuous Control Analytics	Access Control Manager Data Role Transaction Control Manager Data Role
Manage Models		
Update access	Manage Access Models Manage Transaction Models	Access Model Manager Data Role Transaction Model Manager Data Role
View access	View Access Models View Transaction Models	Access Model Manager Data Role Transaction Model Manager Data Role
Create Transaction Model		
Update access	Create Transaction Models	Transaction Model Manager Data Role
View access	View Transaction Models	Transaction Model Manager Data Role
Create Access Model		
Update access	Create Access Models	Access Model Manager Data Role
View access	View Access Models	Access Model Manager Data Role
Manage Access Entitlements		
Update access	Manage Access Entitlements	Entitlement Manager Data Role
View access	View Access Entitlements	Entitlement Manager Data Role
Create Access Global Condition		
Update access	Manage Access Global Conditions	Global Condition Manager Data Role
View access	View Access Global Conditions	Global Condition Manager Data Role
Manage Access Global Conditions		
Update access	Manage Access Global Conditions	Global Condition Manager Data Role
View access	View Access Global Conditions	Global Condition Manager Data Role

Page Access in 8.6.3	Duty Role in 8.6.4	Data Role in 8.6.4
Manage Access Path Conditions		
Update access	Manage Access Path Conditions	Path Conditions Manager Data Role
View access	View Access Path Conditions	Path Conditions Manager Data Role
Manage Participant Groups	(No longer applicable)	(No longer applicable)
Manage Incidents		
Update access	Manage Control Incidents Control Incidents Analytics	Access Incident Manager Data Role Transaction Incident Manager Data Role
View access	View Control Incidents Control Incidents Analytics	Access Incident Manager Data Role Transaction Incident Manager Data Role
Incident Management > Manage Access Approvals		
Update access	Manage Access Approvals	(Not applicable)
View access	View Access Approvals	(Not applicable)
Manage Access Simulations		
Update access	Manage Access Simulations	(Not applicable)
View access	View Access Simulations	(Not applicable)
Manage Users		
Update access	Manage Security	(Not applicable)
View access	View Security	(Not applicable)
Manage Roles		
Update access	Manage Security	(Not applicable)
View access	View Security	(Not applicable)
Manage Application Data		
Update access	Manage Application Datasources Manage Application Libraries	(Not applicable)
View access	View Application Datasources View Application Libraries	(Not applicable)
Manage Application Configurations		
Update access	Manage Application Configurations	(Not applicable)
View access	View Application Configurations	(Not applicable)
Administration Management > Manage Access Approvals		
Update access	Administer Access Approvals	(Not applicable)
View access	View Access Approvals	(Not applicable)
Manage Jobs		
Update access	Manage Jobs	(Not applicable)
View access	View Jobs	(Not applicable)
Manage Schedules		
Update access	Manage Job Schedules	(Not applicable)
View access	View Job Schedules	(Not applicable)
Run Control Reports		
Update access	Continuous Control Reporting	(Not applicable)
View access	Continuous Control Report Viewing	(Not applicable)
Run Incident Reports		
Update access	Control Incident Reporting	(Not applicable)
View access	Control Incident Reporting Viewing	(Not applicable)
Run Access Approvals Reports		
Update access	Control Incident Reporting	(Not applicable)
View access	Control Incident Reporting Viewing	(Not applicable)

Page Access in 8.6.3	Duty Role in 8.6.4	Data Role in 8.6.4
Run GRCC User Reports		
Update access	Security Administration Reporting	(Not applicable)
View access	Security Administration Report Viewing	(Not applicable)
Run Global User Reports		
Update access	Control Incident Reporting	(Not applicable)
View access	Control Incident Reporting Viewing	(Not applicable)
Run Conditions Reports		
Update access	Continuous Control Reporting	(Not applicable)
View access	Continuous Control Reporting Viewing	(Not applicable)

Users

All users, even those who are inactive in 8.6.3, will be upgraded and assigned job roles that are composed of duty and data roles. Each user will have the same access as he or she had prior to the upgrade, with minimal (if any) additional configuration.

During upgrade, each user is assigned a unique value that is used in the Participant Group perspective for security purposes.

Participants

After the upgrade, access to models, controls, and incidents is based on job, duty, and data roles (see *User Guide* for information on security). For increased efficiency, you can associate data roles with values from perspective hierarchies (as described earlier).

A new perspective, called Participant Group, is created during the upgrade. Its values map to the unique values created for users during the upgrade. The perspective values are then assigned appropriately to models, controls, or incidents, to identify the users who had created models, or the users or groups assigned to be participants in controls or incidents. This ensures that users continue to have the same access after the upgrade as they had before.

For example, assume the following setup:

User in 8.6.3	Equivalent in 8.6.4.3000
jsmith (participant)	Group1
ataylor (participant)	Group2
Internal Controls (participant group)	No value assigned in 8.6.4.3000

The intent of the Participant Group perspective is merely to enable users to retain their access under the new security structure. After upgrade, consider phasing out the Participant Group perspective by replacing it with perspectives that make more sense for your company and use the more robust, granular security offered in version 8.6.4.3000.

Because “Group” values, rather than specific usernames, are assigned during the upgrade, a foundation is set for the transition to the new role-based security model. For instance, suppose Group1 is assigned to objects related to the North America region. A more intuitive way to describe Group1, then, would be to rename it “North America.” If Region is the common stratification for the Group values, then the

Participant Group perspective hierarchy could be renamed to "Region," and the generic Group values renamed to the appropriate region values.

Models

In 8.6.3, each model can be accessed only by the person who created it. In 8.6.4.3000, a model is secured with perspectives. This allows greater flexibility in retaining or expanding access to models. During upgrade, a Participant Group perspective value is assigned to each model, corresponding to the user who created the model.

In the example above, if ataylor created a model in version 8.6.3, Group2 would be selected as that model's Participant Group perspective value in 8.6.4.3000.

Controls

In 8.6.3, each control can be accessed by the participants or participant groups associated to it. During upgrade, Participant Group perspective values are assigned to each control, corresponding to users (but *not* groups) that had been assigned as participants to the control.

In the example above, if jsmith and ataylor were assigned as participants to a control in version 8.6.3, Group1 and Group2 would be selected as that control's Participant Group perspective values in 8.6.4.3000.

Incidents

In 8.6.3, incidents can be accessed by the participants or participant groups associated to them. The participants are also represented in the Assigned To column of the Manage Incidents page in version 8.6.3. During upgrade, Participant Group perspective values are assigned to each incident. Each value corresponds to a user assigned as a participant to the incident in version 8.6.3 (but *not* to participant groups).

In the example above, if jsmith and Internal Controls were assigned as participant and participant group for an incident in 8.6.3, then only Group1 would be selected as a Participant Group perspective value for the incident in 8.6.4.3000. (It is assumed that members of the Internal Controls group would have been assigned individually as participants to the control before the upgrade; see "Replace Participant Groups Before Upgrading" on page 1-3. If so, their individual 8.6.4.3000 IDs would be selected as Participant Group perspective values for the incident.)

Note, there is no longer an Assigned To column in the Manage Incident Results grid. To view the participants and participant groups associated to an incident after upgrade, refer to the Participant Group perspective.

The newly added concept of worklists, and their assignment to result investigators, give users greater visibility to what's in their queues than they had in earlier versions.

Data Roles

Data roles define the data level access a user has. During upgrade to 8.6.4.3000, a unique "Group#" is given to each user and each participant group. This "Group#" is then added to a data role, which is assigned to a job role, and ultimately the user. For example:

In 8.6.3, jsmith has a role called Control Manager, with the following access: Manage Controls Update = Allow.

Upon upgrade to 8.6.4.3000, a new data role is created, called *Control Manager – Control Group1 Data Role*.

For each user and role that is upgraded, the following naming convention is used:

[Role] – Control [Group#] Data Role

The following seeded data roles are nested in this new data role:

- Access Control Manager Data Role
- Transaction Control Manager Data Role

The data roles assigned during upgrade are based on the mapping identified in the table beginning on page 1-4.

Also, perspectives called Datasource and Business Object are created. One contains a value for each datasource, and the other for each business object, configured for use with the GRCC instance. This new data role is associated with perspective values for the datasources and business objects to which the user had access in 8.6.3, thus maintaining that access in 8.6.4.3000.

Finally, the Participant Group perspective for this user is included with the new data role: Participant Group = (Group# associated to this data role).

Job Duty Roles

A job duty role is a collection of duty roles. For each existing user and role, a new job duty role is created with the naming convention:

[Role] Job Duty Role

An example would be *Control Manager Job Duty Role*.

The duty roles assigned to the job duty role during upgrade are based on the mapping identified in the table beginning on page 1-4.

Job Roles

Inactive roles are not upgraded in 8.6.4.3000, so be sure to activate any roles in 8.6.3 that are desired for the upgrade. Job roles are created for each user and role combination and have the following naming convention:

[Role][Group#]Job Role

An example would be *Control Manager Group1 Job Role*.

The job role has the job duty role created for a given user and role, as well as each data role created for the user and role. An upgraded user and role might look something like the following:

jsmith:

Control Manager Group1 Job Role:

- Control Manager Job Duty Role (newly created job role; it is a collection of duties)
- Control Manager - Control Group1 Data Role (newly created data role)
- Control Manager - Entitlement Group1 Data Role (newly created data role)

- Control Manager - Model Group1 Data Role (newly created data role)
- Control Manager – Global Conditions Group1 Data Role (newly created data role)
- Control Manager – Path Conditions Group1 Data Role (newly created data role)

Run the Role Assignment Report to view access for users.

Review Security

Review the *Governance, Risk and Compliance User Guide* and *Governance, Risk and Compliance Security Implementation Guide* to become familiar with the role-based access concepts introduced in 8.6.4.3000. With the new job, data, and duty role functionality, consider re-evaluating the existing role structures and perspectives used for data-level access security. As you create perspective hierarchies that make sense for securing your company data, and begin to build out the appropriate data roles, you can phase out the Participant Group perspective and data roles that were used to ensure continued seamless access after the upgrade.

Email Notifications

In 8.6.3, email messages were sent out at a frequency specified in the Notifications tab of the Manage Application Configurations page. For instance, a consolidated email message might be sent to participants of new controls, once a day at 5:00 PM PST. Also, a consolidated email message might be sent to incident participants, showing a listing of controls with pending incidents.

In 8.6.4.3000, consolidated email messages will continue to be sent at a specified frequency, but only to inform result investigators of incidents that require resolution. Each investigator's incidents are also listed in a Worklists tab on his or her home page (the one that opens when the user logs on to GRC) and on a Result Overview page.

A Notifications tab on the home page, and on a Control Overview page, lists controls to which a user's roles provide access, and which have been newly created or modified. Because these do not require action, however, email messages are not sent to alert users to their existence.

Workflow routing has been introduced in 8.6.4.3000. For each control, users with security access to the incidents generated by the control are eligible for selection as a result investigator, to whom worklists should be routed when incident results are generated. Upon upgrade, the investigator associated to each control and to its incident results will by default be set to "All Eligible Users." This means all users who have security access to these controls and incident results will receive worklists.

Manage Access Approvals will continue to send email messages in 8.6.4.3000 as it does in 8.6.3.

After upgrading, consider reviewing controls and assigning a specific user to each as an investigator.

Manage Saved Views

The Manage Saved Views functionality that existed in 8.6.3 is replaced in 8.6.4.3000 by a more robust Search and Saved Search functionality. (See the *User Guide* for more information on this functionality.) Views saved in 8.6.3 need to be re-created, as they are specific to users in 8.6.4.3000. They should be re-evaluated to be optimized for each user's specific requirements.

The following screens will retain their existing search capability, but will not offer an option to save searches in 8.6.4.3000:

- GRCC Manage Access Global Conditions
- GRCC Manage Access Approvals
- GRCC Manage Access Approvals Administration
- GRCC Manage Jobs
- GRCC Manage Application Data (Datasources tab)
- GRCC Manage Application Data (Business Objects tab)

Scheduled Reports

Reports have been enhanced to allow for report parameters to be saved. Previous to 8.6.4.3000, report parameters were based on a "saved view," which was tied to views used in the Manage Controls or Manage Incident screens. In 8.6.4.3000, the more robust saved report parameters are unique per user and per report and should be re-evaluated to be optimized for each user's specific requirements. This includes rescheduling any reports that had been scheduled in 8.6.3.

Tags Converted to Perspectives

In 8.6.3, tags were used to categorize records. They could be used as parameters in searches; the resulting set of records would be displayed in management pages or reports. In 8.6.4.3000, tags have been converted to perspectives. The benefits of tags are still realized with perspectives, but perspectives are more powerful. Perspectives allow for data-level security, and a multilevel tree structure. (See the *User Guide* for more information on this functionality.)

Inactive tags and tag values are not upgraded in 8.6.4.3000, so be sure to activate any tags in 8.6.3 that are desired for upgrade.

Also note, in 8.6.3, tags and tag values could exceed 150 characters. With the upgrade to 8.6.4.3000, the perspectives and perspective values into which they are converted will be truncated to 150 characters. For each, the perspective description will show the entire string. However, before upgrading you may want to be sure your tag and tag values do not exceed 150 characters.