An Oracle White Paper
December 2018

Granular Security for Assessments in Financial Reporting Compliance

Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Overview

Beginning with Release 13 Update 18C, data security for Financial Reporting Compliance assessments is no longer dependent on data security for other objects.

In Financial Reporting Compliance, data security policies determine which items are available to users. The policies are mapped to roles, which are in turn assigned to users. A policy may specify perspective values. If so, a user subject to the policy can see only items assigned the same perspective values.

In updates prior to 18C, risks, controls, and processes were the only items assigned perspective values, and so the only items secured directly by data security policies. Assessments of these objects inherited data security from the objects themselves.

An individual process, risk, or control may be assigned multiple perspective values. In such a case, an assessment of the item could be completed by a user whose data security policy matched any value selected for the item. For example, a control might be assigned two values — North and South — of a perspective called Region. An assessor from either region could assess the control. Although assessment criteria might differ in the two regions, one assessor assigned the North value and another assigned the South value could not perform independent assessments.

Beginning with Update 18C, however, data security for batch assessments is enforced separately from data security for the objects being assessed. You configure data security for assessments as you create assessment plans. You can, therefore, document a given process, risk, or control once, but create multiple assessments for it. Each assessment would correspond to one of the perspective values assigned to the item, and each would be independent of the others.

In the example, an assessor from the North region could complete one assessment of the control, and an assessor from the South region could complete a separate assessment of the control. Neither would have access to the other's information.

To take advantage of this enhancement, however, you must update the roles and data security policies your company currently uses.

Updating Roles and Data Security Policies

To implement the new assessment capability, update data security policies so that assessment duties are associated with perspective values.

Job and duty roles grant access to functionality. A job role conceptually represents a job a user would perform in an organization. It provides broader functional access than a duty role, which represents one or more tasks included within a job. In a typical implementation, you create job roles, but you use predefined duty roles as their components.

We're concerned with job roles that grant assessment rights — either specifically or in combination with other rights. Typically, such a job role contains:

- A duty role that enables you to work with a type of object — with processes, risks, or controls. For a job role devoted specifically to assessment, this would be a duty role that grants view rights. For a more general-purpose job role, this would be a duty role that grants create or edit rights.
- A duty role that grants rights to assess objects, set up assessments, review them, or approve them.

Duty roles map to data security policies. If your job role uses predefined duty roles, however, these are already mapped to predefined data security policies, and you don't need to modify the duty-level policies.

You do, however, need to ensure that the job role maps to a single data security policy that contains the following filters:

- One filter selects the data security policy that applies to the object-rights duty role you included in your job role.
- A second filter selects the data security policy that applies to the assessment duty role you included in your job role.
- A third filter selects a specific perspective value. The user assigned the job role can therefore see, and assess, only records of items assigned that value.

In a typical configuration for updates earlier than 18C, the job-level data security policy would omit the filter that selects the policy mapped to the assessment duty role. To update the job-level policy for 18C, you would add that filter.

In our example:

- You might create a job role called "Control Assessor North." It includes the Control Viewer Composite duty role and the Control Operational Assessor Composite duty role. Because it uses the Viewer duty role, this would be appropriate for a user who assesses controls, but does not work with them in other ways.
- You would map the job role to a data security policy that contains three filters. One selects the Control Viewer data security policy, and the second selects the Control Operational Assessor data security policy. The third filter would select a value of the Region perspective — in this case, North. So a person granted the job role can assess only controls assigned the North perspective value.
- You would create a second job role that contains the same duty roles. Call it "Control Assessor South." You would map it to a data security policy that is identical to the North policy except that its perspective filter selects the South value rather than the North value. A person granted the job role can assess only controls assigned the South perspective value.

Applying Granular Data Security to Batch Assessments

To set up batch assessments, you first create a template. You then develop a plan from the template, and then initiate a batch of assessments from the plan. You configure granular data security for the assessments while you create the plan.

Broadly, as you create a template, you select a "primary object" of assessment — Process, Risk, or Control. As you develop a plan from the template, you may assign a survey to be completed during assessments, and you configure criteria for selecting instances of the primary object to be assessed.

Among those selection criteria, you may assign perspective values to the assessment batch. (One option is to assign no values.) In earlier updates, this was a relatively simple process: assessors (or assessment reviewers or approvers) could participate in an assessment only if their assessment roles mapped to data security policies that specified at least one of those perspective values.

Update 18C is more flexible. In a Perspective Selection and Assignment Criteria region of the page to create assessment plans:

- A No Perspectives check box is selected by default. If you leave it selected, make no further selections in this region. The assessments then include only items assigned no perspective values. Clear this check box if you want to assess items that are assigned perspective values.
- If you clear the No Perspectives check box, click Add to open a Select Perspective Criteria dialog. In it, select a perspective hierarchy and any number of values from it. Repeat this to select values from as many hierarchies as you like. Assessments generated from the plan then include only instances of the primary object associated with the selected values.

  If you select from two or more perspective hierarchies, their values have an AND relationship. That means items selected for assessment must be associated with the values selected from each of the perspective hierarchies.
- If you have selected perspective values, select or clear an Include Duplicate Records check box. If you select it, multiple assessments are generated for each instance of the primary object — one for each of the perspective values it's assigned. An assessor (or reviewer or approver) has access only to assessments with perspective values that match those in his or her data security policies.

  If you clear the check box, a single assessment is generated for each instance of the primary object and all the perspective values assigned to it. An assessor has access to the assessment if his or her data security policies contain any of those perspective values. In effect, this option causes the assessment plan to behave as assessment plans did in updates of Financial Reporting Compliance earlier than 18C.

In our example:

- The template selects Control as the primary object. As you create a plan, you clear the No Perspectives check box and select the North and South values of the Region perspective hierarchy.
- If you select the Include Duplicate Records check box, the initiate-assessment job creates two assessments for each qualifying control. One is assigned the North perspective value and so is available to assessors whose data security policies specify only the North value, or both the North and South values. The other is assigned the South perspective value and so is available to assessors whose data security policies specify only the South value, or both the North and South values.
- If you clear the Include Duplicate Records check box, the initiate-assessment job creates one assessment for each qualifying control. It is available to assessors whose data security policies specify either or both of the North and South values.

Additional Information

For more information:

- See *Implementing Risk Management* to learn about creating and managing perspective hierarchies.
- See *Securing Risk Management* for detailed procedures for creating roles, creating data security policies, and mapping them to one another.
- See *Using Financial Reporting Compliance* for detailed discussions of setting up and completing assessments.

These guides are available in the Oracle Help Center (docs.oracle.com). From the home page of the Help Center, follow this path: Cloud > Applications > Risk Management (under Enterprise Resource Planning) > Books.

Granular Security for Assessments in Financial Reporting Compliance
December 2018

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200

oracle.com

Oracle is committed to developing practices and products that help protect the environment

Hardware and Software, Engineered to Work Together