# Oracle® Fusion GRC Intelligence

User Guide

Release 8.6.4.7000

**Part No. E40669-01**

May 2013

ORACLE

Oracle Fusion GRC Intelligence User Guide

Part No. E40669-01



Primary Author: David Christie

# Contents

## GRC Intelligence

# Preface

This Preface introduces the guides and other information sources available to help you more effectively use Oracle Fusion Applications.

## Disclaimer

The information contained in this document is intended to outline our general product direction and is for informational sharing purposes only, and should be considered in your capacity as a customer advisory board member or pursuant to your beta trial agreement only. 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 in this document remains at the sole discretion of Oracle. This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle software license and service agreement, which has been executed and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

## Other Information Sources

### My Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/support/contact.html or visit http://www.oracle.com/accessibility/support.html if you are hearing impaired.

Use the My Oracle Support Knowledge Browser to find documents for a product area. You can search for release-specific information, such as patches, alerts, white papers, and troubleshooting tips. Other services include health checks, guided life cycle advice, and direct contact with industry experts through the My Oracle Support Community.

## Oracle Enterprise Repository

Oracle Enterprise Repository provides visibility into service-oriented architecture assets to help you manage the life cycle of your software from planning through implementation, testing, production, and changes. In Oracle Fusion Applications, you can use the Oracle Enterprise Repository for:

- Technical information about integrating with other applications, including services, operations, composites, events, and integration tables. The classification scheme shows the scenarios in which you use the assets, and includes diagrams, schematics, and links to other technical documentation.
- Publishing other technical information such as reusable components, policies, architecture diagrams, and topology diagrams.

The Oracle Fusion Applications information is provided as a solution pack that you can upload to your own deployment of Oracle Enterprise Repository. You can document and govern integration interface assets provided by Oracle with other assets in your environment in a common repository.

# Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/us/corporate/accessibility/index.html.

# Comments and Suggestions

Your comments are important to us. We encourage you to send us feedback about Oracle Fusion Applications Help and guides. Please send your suggestions to oracle_fusion_applications_help_ww@oracle.com. You can use the Send Feedback to Oracle link in the footer of Oracle Fusion Applications Help.

# GRC Intelligence

Oracle Fusion GRC Intelligence (GRCI) provides dashboards and reports that present summary and detailed views of data generated in Oracle Enterprise Governance, Risk and Compliance (GRC).

GRC, in turn, serves as a platform for several applications — Enterprise Governance, Risk and Compliance Manager (EGRCM), Application Access Controls Governor (AACG), and Enterprise Transaction Controls Governor (ETCG).

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 to which risks and controls apply.

AACG and ETCG enable users to create models and 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."

These components run as modules in the GRC platform. AACG and ETCG run as a Continuous Controls Monitoring (CCM) module. EGRCM provides a Financial Governance module by default, and users may create other EGRCM modules to address other areas of the company's business.

GRCI may be installed in an embedded mode within GRC, or it may run as a standalone application on an OBIEE server.

In embedded mode, GRCI provides an Intelligence tab that is available from the GRC home page or from overview pages for GRC objects. Dashboards are available from "subtabs" of the Intelligence tab. Each dashboard displays a set of reports that provide broad graphic and tabular views of data. From each report, you can "drill down" to other reports that provide more detailed and focused views.

## Viewing GRCI

Several factors determine which dashboards are available to you. These include the GRC components your company has implemented, the dashboards selected for use during GRC configuration, and the rights granted by your GRC job roles.

Seeded GRC job duty roles lead to privileges that enable a user to access GRCI dashboards and reports from particular locations within GRC. Each of these job duty roles contains the phrase "Embedded Intelligence Viewer," and the name of each also indicates the location from which dashboards and reports may be viewed. For example, the Risk Embedded Intelligence Viewer Job Duty Role provides access to the Intelligence tab from the overview page for EGRCM Risk Management. Or, the CCM Embedded Intelligence Viewer Job Duty Role provides access to CCM dashboards and reports from the home page.

To view GRCI dashboards in GRC, you must be assigned a job role that incorporates appropriate job duty roles — one or more of the seeded Embedded Intelligence Viewer job duty roles, or job duty roles created to lead to the same privileges as these roles.

In addition, data roles may limit the content of the dashboards to which you have access.

For more on selecting dashboards for use, see the *Enterprise Governance, Risk and Compliance Installation Guide*. For more on data, duty, and job roles, see the *Enterprise Governance, Risk and Compliance User Guide* and the *Enterprise Governance, Risk and Compliance Security Implementation Guide*.

# Using Dashboards

GRCI is, in effect, an instance of Oracle Business Intelligence Enterprise Edition (OBIEE) configured both to report on GRC data and to be embedded within GRC. See OBIEE documentation for information on creating custom reports and customizing dashboards. Features available in the default GRCI dashboards include the following.

## Dashboard Filters

Each dashboard page is displayed from a subtab of the Intelligence tab. A dashboard may include page-parameter LOVs, in which you can select values. Within a given dashboard, reports focus on the values you select in these LOVs.

For EGRCM dashboards, these values include time (year or quarter) and perspectives. A perspective is a hierarchical representation of a context in which objects exist. An Organization perspective, for example, might map the structure of a company that implements GRC; this would enable the company to associate individual risks, controls, or other objects with divisions, units, or other corporate entities to which they apply.

Thus in a dashboard for EGRCM reporting, you might select Organization for perspective hierarchy and 2013 for year. Reports would show only data pertaining to objects assigned some value in the Organization perspective, and current in 2013. Or you might select North American Division (assuming this value exists in your Organization hierarchy) and first quarter of 2013 to focus results further.

In CCM dashboards, filtering values include control type (access or transaction), datasource, eligible investigator, and incident status. A datasource is an instance of a business application subject to CCM controls. Incidents are records of control violations; "result investigators" review incidents; as they do, they assign any of several statuses to them.

In addition to setting filters, you can expose or hide reports within a dashboard by selecting the ± toggle at the upper-left corner of each report.

## Drill Down

Typically, a primary GRCI report provides a graph and a table that displays values depicted in the graph. (A "primary" report is one of those available by default in a subtab of the Intelligence tab.)

If you position the mouse cursor over a shape in a graph — a line, a bar in a bar graph, or a "slice" of a pie chart — GRCI displays the data represented by that shape.

For example, a Compliance Status Report includes a bar chart in which each bar represents a count of certified assessments, or of issues, associated with a specified perspective. (Assessments and issues are discussed more fully later in this document.) When you move the mouse cursor over a bar, a message states the item being counted (certified assessments or issues), the value of the count, and the perspective to which the count applies.

Moreover, you can select a shape within a graph to open a subsidiary report that provides detail about your selection. For example, from the Compliance Status report, you can select the bar representing a certified assessment count to open a Certification Detail Report. Or you can select a bar representing an issue count to open an Issue Detail report. The subsidiary report presents information about the shape you select — in this case, certification details or issue details for a specific perspective.

You can open the same subsidiary reports by selecting hyperlinked (blue-colored) values within the table that accompanies a graph in a primary report. To use the Compliance Status Report as an example once again, its table includes Hierarchy Name, Certified Assessment Count, and Issue Count columns whose values are links to subsidiary reports. Selecting a value in the Certified Assessment Count column opens the Certification Detail Report; selecting a value in the Issue Count column opens the Issue Detail Report.

If you were to select a perspective hierarchy in the Hierarchy Name column, the result would be a fresh rendering of the primary report (in this example, Compliance Status) that includes only information about the perspective hierarchy you select.

To select any element in a primary report:

1. Click on the element you want to select. A label appears, showing the name of the subsidiary report you are about to open.
2. Click on the label to open the subsidiary report.

# EGRCM Dashboards

Three Intelligence subtabs — Certifications, Issues, and Analysis — apply to EGRCM.

- Users may periodically assess objects to determine that they are defined and implemented correctly when they are created, or that their definition and implementation remain appropriate as time passes. There are several assessment types, one of which is "Certification." GRCI reports on the Certifications tab concern the status of assessments.
- Reports on the Issues tab concern defects or deficiencies that EGRCM users detect either in objects or in activities being performed against objects, such as an assessment, risk analysis, or risk evaluation.
- Reports on the Analysis tab provide data about controls.

GRCI reports provide information about controls, risks, or other EGRCM objects, and about issues raised against these objects, but frequently organize results by the perspective with which these objects are associated.

## Certifications Dashboard

Click on the Certifications subtab to view the following reports:

- Compliance Status: This report displays information about assessments whose assessment-activity type is Certification. The graph presents pairs of bars, each of which applies to Certification assessments of objects associated with a specified perspective hierarchy. In each pair, the height of one bar shows the number of complete assessments, and the other shows the number with issues. Both the graph and the table show current values, and the table compares current certifications with the previous month's.
- Overdue Assessments: This report shows numbers of assessments that are (or are not) behind schedule. Each bar in the graph represents a range of days overdue, including one bar that represents "not yet due." The height of each bar is proportional to the number of assessments within its category. The table provides additional information: the name of each overdue assessment, its due date, the process to which it belongs, and the perspective hierarchy with which it is associated.
- Control Assessments Results: This report shows numbers of controls that have passed and failed assessment. Each bar in the graph represents controls associated with a specified perspective hierarchy; each includes a segment for passed controls and another for failed controls. The table contains a row for each assessment in which controls have passed or failed (and a given control may be included in any number of assessments). It displays the total number of controls in each assessment, the numbers (and percentages) of passed and failed controls, and the perspective hierarchy with which the assessment and its controls are associated.

## Issues Dashboard

Click on the Issues subtab to view the following reports:

- Open Issues by Severity: As issues are created, they may be assigned labels that rate their severity. Each bar in the graph represents issues at a given severity, and each includes a segment representing total issues and a segment representing open issues. The graph may contain a bar with no severity label; if so, it represents issues that have not been assigned any severity.

  In the table, each row displays counts of issues at a given severity, raised against objects associated with a specified perspective hierarchy. (A given issue may apply to an object associated with more than one hierarchy, so tabular counts for any severity may appear to add up to more than those shown in the graph.)
- Issues by Likelihood of Recurrence: As issues are created, they may be assigned labels that rate their likelihood of recurring — for example high, medium, or low. Each bar in the graph represents issues at a given likelihood. Each includes a segment representing total issues and a segment representing open issues. The graph

may contain a bar with no likelihood label; if so, the bar represents issues that have not been assigned any likelihood.

In the table, each row shows counts of issues at a given likelihood, associated with a particular perspective hierarchy, assessment, and risk. (Again, a given issue may apply to an object associated with more than one of each of these items, so tabular counts for any likelihood may appear to add up to more than those shown in the graph.)

- Impact of Issues: Users may assign an impact value to each issue in EGRCM. In the graph for this report, each bar represents the number of issues within an "impact cost category" — a range of cost percentiles. The "0.75–1" category, for instance, represents the number of issues above the seventy-fifth percentile. The graph may contain a bar with no cost-category label; if so, it represents an issue for which no impact cost has been assigned.

  In the table, each row shows an issue and the process, risk, and control it affects. (An issue may apply to more than one or each of these items, so the table may contain more rows than the number of issues in the graph). Each row also shows the perspective hierarchy with which an issue is associated and its impact cost.

- Issues by Certifications in Progress: This report compares the number of issues to the number of open issues raised in assessments of the Certification type. Each bar in the graph represents issues raised against objects associated with a given perspective hierarchy. The table shows the number of Certification assessments for objects associated with each perspective, as well as the total and open issue counts for those assessments.

## Analysis Dashboard

Click on the Analysis subtab to view the following reports:

- Control Count Trend: This report shows the change in the number of controls implemented as time passes. The graph is a linear track of control counts from one period to the next. The table shows the controls created from one period to another. You can drill from year to quarter to month.

- Controls by Risk Type: Each risk is assigned a type value. Each control is created to address one or more risks. This report shows the number of controls created for each risk type. The graph includes a bar for each risk type, the height of which corresponds to the number of controls. The table includes a row for each risk type within each perspective hierarchy, showing the number of controls and the percentage that value is over the number for the previous period.

- Risk Level Reduction: Risks may be associated with analysis models which (in concert with other models) calculate the likelihood that a risk event will occur, the impact if it does, and an overall risk value. Moreover, model results may be considered "inherent" (no controls exist to mitigate risk), "residual" (controls exist to mitigate risk), or "target" (a treatment plan exists to mitigate risk).

  This report presents the effect of control types in reducing risk. Bars represent the inherent, residual, and target levels by risk type, and the table presents corresponding data.

### Subsidiary EGRCM Reports

By drilling down from these EGRCM primary reports, you can open the following reports:

- Assessment Detail: Displays all the details related to a set of assessments.
- Assessment Activity Detail: Displays all details related to a set of activities included in an assessment.
- Certification Detail: Displays all the details related to a set of Certification activity assessments.
- Control Detail: Displays all the details configured for a set of controls.
- Issue Detail: Displays all the details related to a set of issues.
- Risk Detail: Displays all the details related to a set of risks.

## CCM Dashboards

Four Intelligence subtabs apply to AACG and ETCG: CCM Control Overview, Incident Status, Incident Summary, and User Access Review.

Users may create "continuous controls." These either define conflicts among duties that can be assigned in a company's applications, or define ways in which transactions entail risk. Continuous controls generate "incident results" — records of transactions, or users with access, that continuous controls define as risky. Access analysis may be "preventive" — it may grant, deny, or require approval for role assignments that violate controls created before the assignments were made.

GRCI reports provide information about continuous controls, the incidents they generate, the status assigned to those incidents by result investigators, and the status of users and their role assignments.

### CCM Control Overview Dashboard

Click on the CCM Control Overview subtab to view the following reports:

- Control Summary by Datasource: In a pie chart, each "slice" represents a count of the controls on a datasource that is subject to CCM continuous controls.
- Control Summary by Control Type: In a pie chart, each "slice" represents a count of the controls by type — Access or Transaction.
- Control Summary: A table includes a row for each datasource, displaying its control count.

### Incident Status Dashboard

A status may be assigned to an incident at various stages. Incident statuses include the following:

- Assigned: An incident has been generated, and one or more investigators are assigned to review it.
- Remediate: An investigator determines that some action must be taken to resolve the incident.

- Resolved: An investigator confirms that remedial action has been taken.
- Pending: This is not a formal status, but an incident is considered to be pending when it is initially generated (at the Assigned status) or if a user sets its status to Assigned or Remediate and then submits the change.
- Accepted: An investigator determines that nothing need be done to resolve the incident.
- Authorized: Preventive analysis causes a role assignment to be suspended, an investigator approves the assignment, and the control is subsequently evaluated.
- Control Inactive: An incident is no longer of concern because the control that generated it has been inactivated.
- Closed: An incident has been resolved in its business application, and a subsequent evaluation of controls finds that the incident need no longer be addressed.
- Rejected: Preventive analysis required approval for a role to be granted, and approval was denied.
- Prevented: Preventive analysis automatically denied access to a role.
- Approved: Preventive analysis automatically granted access to a role.

Click on the Incident Status subtab to view the following reports:

- Incident Summary by Status: A pie chart is divided into slices, each of which represents the number of incidents at a given status. A table shows the number of incidents generated by each control, at each status.
- Incident Summary by Age: In a pie chart, each slice represents the number of pending incidents that have existed for a range of days. For each range, a table shows the number of pending incidents.

## Incident Summary Dashboard

Click on the Incident Summary subtab to view the following reports:

- Incident Summary by Datasource: A pie chart is divided into slices, each of which represents the number of pending incidents existing on one of the datasources subject to CCM controls. A table displays the number of pending incidents associated with each datasource.
- Incident Summary by Control: A pie chart is divided into two slices. One represents the number of pending access incidents, and the other the number of pending transaction incidents. A table shows the number of pending incidents generated by each control of one type or the other — access or transaction.

## User Access Review Dashboard

Click on the User Access Review subtab to view the following reports:

- List of Roles Accessible by Users: This report lists users of business applications subject to CCM controls, and shows the roles assigned to each within those applications.
- List of Users By Role: This report lists roles available in business applications, and then lists the users assigned each role (together with start and end dates for each assignment).

### Subsidiary CCM Reports

By drilling down from CCM primary reports, you can open the following reports:

- Control Listing: Displays details of controls.
- Incident Listing Report: Provides details of incidents.
- Incidents by User: Displays incident information by user.
- Incidents by User, Role: Displays incident information by user and role.

## Standalone Reports

When configured as an independent instance of OBIEE with GRC data, GRCI provides the following additional reports.

For EGRCM:

- Assessment Cycle Time: Displays the cycle time from start to end for each assessment.
- Control Analysis by Perspectives: Displays controls with various attributes for each organization.
- Control Test Results: Displays the test results for controls.
- Issue Remediation Cycle Time: Displays the cycle time for remediating open issues.
- Process Detail: Displays all the details related to a set of objects.
- Risks by Open Issues: Displays the risks associated with each open issue.
- Treatment Cost Benefit: Displays the cost and benefit of each risk treatment.
- UDA Mapping: Enables the user to understand the mapping for user-defined attribute values and metadata.

For CCM, Incident Burndown: The count of the current pending incidents generated by each control, compared with the count for the previous month.

These reports may be modified or included in GRCI dashboards. Again, see OBIEE documentation for information on creating custom reports and customizing dashboards.