Oracle® Fusion Governance, Risk and Compliance Intelligence

User's Guide

Release 2.0.1

Part No. E14615-01

April 2009

ORACLE®

Oracle Fusion Governance, Risk and Compliance Intelligence User's Guide, Release 2.0.1

Part No. E14615-01

Contents

3   Application Access Control Dashboards

4   Repository Modeling for SOD Subject Areas

A Modifying Reports and Dashboards

Index

Send Us Your Comments

Oracle Fusion Governance, Risk and Compliance Intelligence User's Guide, Release 2.0.1

Part No. E14615-01

Oracle welcomes customers' comments and suggestions on the quality and usefulness of this document. Your feedback is important, and helps us to best meet your needs as a user of our products. For example:

- Are the implementation steps correct and complete?
- Did you understand the context of the procedures?
- Did you find any errors in the information?
- Does the structure of the information help you with your tasks?
- Do you need different information or graphics? If so, where, and in what format?
- Are the examples correct? Do you need more examples?

If you find any errors or have any other suggestions for improvement, then please tell us your name, the name of the company who has licensed our products, the title and part number of the documentation and the chapter, section, and page number (if available).

Note: Before sending us your comments, you might like to check that you have the latest version of the document and if any concerns are already addressed. To do this, access the new Applications Release Online Documentation CD available on My Oracle Support and www.oracle.com. It contains the most current Documentation Library plus all documents revised or released recently.

Send your comments to us using the electronic mail address: appsdoc_us@oracle.com

Please give your name, address, electronic mail address, and telephone number (optional).

If you need assistance with Oracle software, then please contact your support representative or Oracle Support Services.

If you require training or instruction in using Oracle software, then please contact your Oracle local office and inquire about our Oracle University offerings. A list of Oracle offices is available on our Web site at www.oracle.com.

Preface

Intended Audience

Welcome to Release 2.0.1 of the *Oracle Fusion Governance, Risk and Compliance Intelligence User's Guide.*

This guide is intended for information technology personnel and privileged users responsible for using and configuring the GRC Intelligence application. It assumes the reader is familiar with Oracle applications.

See Related Information Sources on page x for more Oracle Applications product information.

Deaf/Hard of Hearing Access to Oracle Support Services

To reach Oracle Support Services, use a telecommunications relay service (TRS) to call Oracle Support at 1.800.223.1711. An Oracle Support Services engineer will handle technical issues and provide customer support according to the Oracle service request process. Information about TRS is available at http://www.fcc.gov/cgb/consumerfacts/trs.html, and a list of phone numbers is available at http://www.fcc.gov/cgb/dro/trsphonebk.html.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible to all users, including users that are disabled. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at

http://www.oracle.com/accessibility/.

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

Structure

1 **Dashboards**
2 **Governance and Compliance Management Dashboards**
3 **Application Access Control Dashboards**
4 **Repository Modeling for SOD Subject Areas**
A **Modifying Reports and Dashboards**

Related Information Sources

Oracle Fusion Governance, Risk and Compliance Intelligence, Implementation Guide, Release 2.0.1 Part No. E14616-01

Do Not Use Database Tools to Modify Oracle Applications Data

Oracle STRONGLY RECOMMENDS that you never use SQL*Plus, Oracle Data Browser, database triggers, or any other tool to modify Oracle Applications data unless otherwise instructed.

Oracle provides powerful tools you can use to create, store, change, retrieve, and maintain information in an Oracle database. But if you use Oracle tools such as SQL*Plus to modify Oracle Applications data, you risk destroying the integrity of your data and you lose the ability to audit changes to your data.

Because Oracle Applications tables are interrelated, any change you make using an Oracle Applications form can update many tables at once. But when you modify Oracle Applications data using anything other than Oracle Applications, you may change a row in one table without making corresponding changes in related tables. If your tables get out of synchronization with each other, you risk retrieving erroneous information and you risk unpredictable results throughout Oracle Applications.

When you use Oracle Applications to modify your data, Oracle Applications

automatically checks that your changes are valid. Oracle Applications also keeps track of who changes information. If you enter information into database tables using database tools, you may store invalid information. You also lose the ability to track who has changed your information because SQL*Plus and other database tools do not keep a record of changes.

1

Dashboards

About Dashboards

GRC Intelligence provides dashboards that present a summarized view of key information such as significant account evaluations and certification results, by significant account, organization, and process. The dashboards highlight potential trouble areas such as ineffective controls, processes that are certified with issues, and unmitigated risks.

Dashboards and the reports contained on them are fully customizable. To customize a dashboard, select Edit Dashboard from the Page Options menu. Once on the Edit Dashboard page, refer to the online help for detailed information on editing the dashboard

Many dashboards also have page-level prompts that you can use to view all reports on the dashboard by Period Name, Control Type, Issue Type, Risk Type, Process Type, or Assessment Type..

Dashboard Options

On every report on all dashboards, you have the following options:

- **Modify:** Select to customize the current report. After you select the Modify link, refer to the online help for details on modifying the report.

- **Refresh:** Select to update the report with the most current data.

- **Download:** Select to download the current report to Excel, Powerpoint, Excel 2000, Data, or to a Web Page (MHTML)

- **Add to Briefing Book:** If your organization licensed Oracle BI Briefing Books, select this link to store a static snapshot of dashboard pages or individual requests in one or more briefing books. You can then download and share briefing books for

viewing offline.

You can choose to view many GRCM reports by the following dimensions:

- **Account Level:** The level of the account hierarchy used to model the account structure of an organization.

- **Cycle level:** The level of the cycle hierarchy used to model the business cycle structure of an organization, such as payroll.

- **Organization level:** The level of the organizational hierarchy structure.

- **Fourth Map level:** The level of an optional organizational hierarchy structure. The fourth hierarchical data map is not configured by default; it is user-defined.

In many reports you can select a process, issue or risk to view details in GRC Manager. GRC Manager works with different roles and responsibilities in compliance with the Sarbanes-Oxley Act to enable users to perform the following types of tasks in managing business process information:

- Create organization maps and business processes

- Define assertions, risks, controls and tests for controls for business processes

- Route business processes for data collection, approval, management assessment, and testing

- Revise, validate, and approve business processes

- Test controls for business processes and document the test results

- Create, remediate and close issues associated with business processes

- Generate and review reports

- Monitor compliance status via the Executive Dashboard

# 2

Governance and Compliance Management Dashboards

This chapter covers the following topics:

- GRC Overview Dashboard
- Certifications Dashboard
- Controls Dashboard
- Issues Dashboard
- Risks Dashboard
- Audit Testing Dashboard
- Audit Planning Dashboard
- Oracle BI Publisher (BIP) Reports

GRC Overview Dashboard

The GRC Overview Dashboard consists of two tabs:

- Overall
- Activities
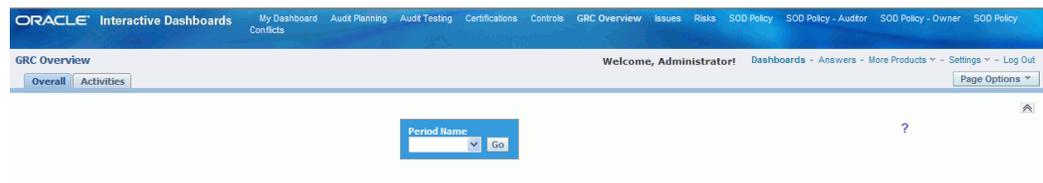
GRC Overall Tab

The GRC Overall tab consists of the following reports by default, but you can customize the page to add custom reports if desired. You can also specify a period, which will limit the data shown in all of the reports on the dashboard to that specific period.

- **Risk Heat Map - Business Processes:** Highlights risk significance and likelihood by Business Process. Select the Number of Processes to view details about the processes.
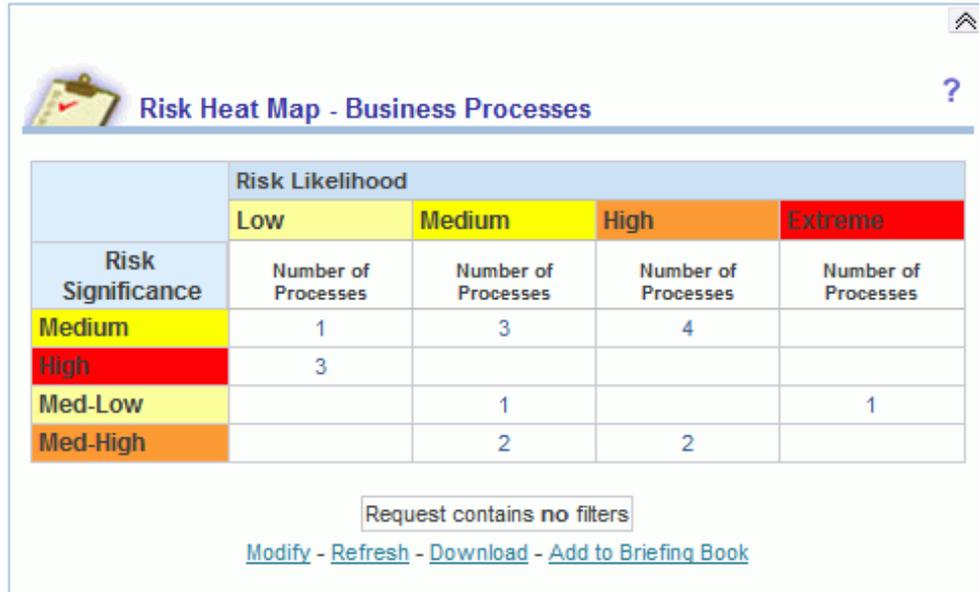
- **High Risk Processes - Heat Map:** This is a landing report for Risk Heat Map - Business Processes. After clicking the count of processes, you view the detail report as shown below.

GRC Overview

### High Risk Processes - Heat Map   ?

Control Type	Process Type	In Scope	Process Title	Process Document ID	Risk Significance	icadmin Risk Rating Low
Preventive	Process	No	Payroll - VL	589	Medium	6
		No	Payroll - VL	597	Medium	6
		No	Payroll - VL	628	Medium	6
		No	Payroll - VL	671	Medium	6
		No	Payroll - VL	692	Medium	6
		No	Payroll - VL	701	Medium	6
		No	Payroll - VL	703	Medium	6
		No	Payroll - VL	706	Medium	6
		No	Payroll - VL	707	Medium	6
		No	Payroll - VL	720	Medium	6
		No	Payroll - VL	723	Medium	6
		No	Payroll - VL	728	Medium	6
		No	Payroll - VL	745	Medium	6
		No	Payroll - VL	781	Medium	6
		No	Payroll - VL	786	Medium	6
		Yes	AP3	894	Medium	6

Return – Modify – Refresh – Download – Add to Briefing Book – Create Bookmark Link

This report lists the process title, document id's with the risk significance and risk rating values.

- **Risk Heat Map - Process Issues:** Highlights risk significance and likelihood by Process Issue.
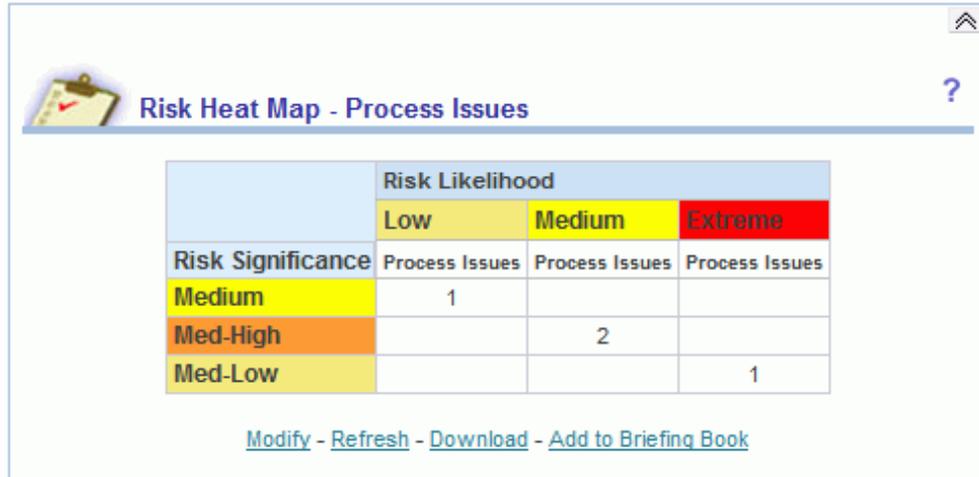
- **Risk Heat Map - Controls:** Highlights risk significance and likelihood by Control. Drill down in the Control type column to see details broken down by type (Preventive, Corrective or Detective.) Drill down in a Number of Controls column to see additional details.

  Note: The note you see on the report in this example is due to a filter that was applied when the report was created. The data within the filter is test data and is not applicable to your implementation. Refer to Appendix A of this guide for additional information on filters.

- **Control Detail - Control Count:** This is a landing report for Risk Heat Map - Controls. After clicking count of controls, you view the detail report as shown below.


This is a detail report on control. It includes control name, type, control document id. It also identifies the scope of the control to see if the control is currently in scope or not.

- **Risk Heat Map - Control Issues:** Highlights risk significance and likelihood by Control Issue. Drill down in a Control Issues column to see details of the control issues including whether or not the control is in scope, the risk significance and the risk likelihood.
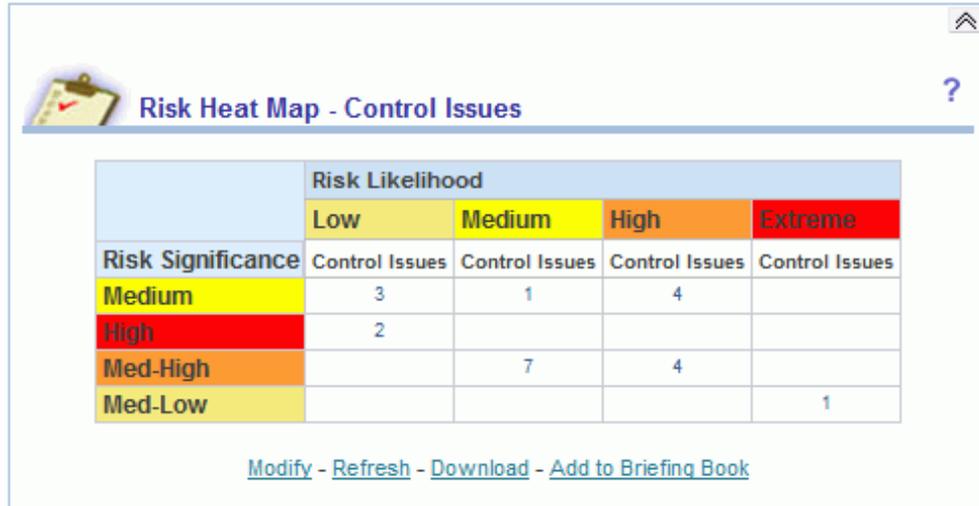
- **Control Detail - Control Issue Count:**This is a landing report for Risk Heat Map - Control Issues. By clicking the count of controls having issues, the detail report Control Detail - Control Issue Count appears. This report contains all the control details along with the risk and control issue counts.

- **Regulatory Compliance Status:** Displays the overall compliance status. Drill down to see details of the controls including how many failed controls there are by period. You can view this report by Account level, Cycle level, Organization level, or Fourth Map level.

  In Scope: The "In Scope" field, with its Yes/No option, is used to indicate whether or not a control is in scope for testing.

  Failed Control Count: The "Failed Control Count" field illustrates the number of controls that failed. There cannot be a failed control count, if there are no tests attached to a control. The total control count and the failed control count are used to calculate failed control count percentage (Failed Control %). Failed Control Count percentage = Failed Control Count * 100 / Total Control Count.

- **Certification Status:** Shows the number of certified processes by account and by process. You can view this report by Account level, Cycle level, Organization level, or Fourth Map level. You can also select a process document ID or dimension value to view additional details.

- **Non-Compliant Processes:** Displays noncompliant processes. You can view this report by Account level, Cycle level, Organization level, or Fourth Map level. Select a dimension value to view additional details.

GRC Activities Tab

The GRC Activities tab consists of the following reports by default, but you can customize the page to add custom reports if desired. You can also choose to limit the reports by Period, Control Type, Issue Type, Process Type, Risk Type, and Assessment Type using the dashboard prompts.

- **Action Items Summary:** Shows the status and the count of Action Items for an Organization, Process or Account based on selected criteria.
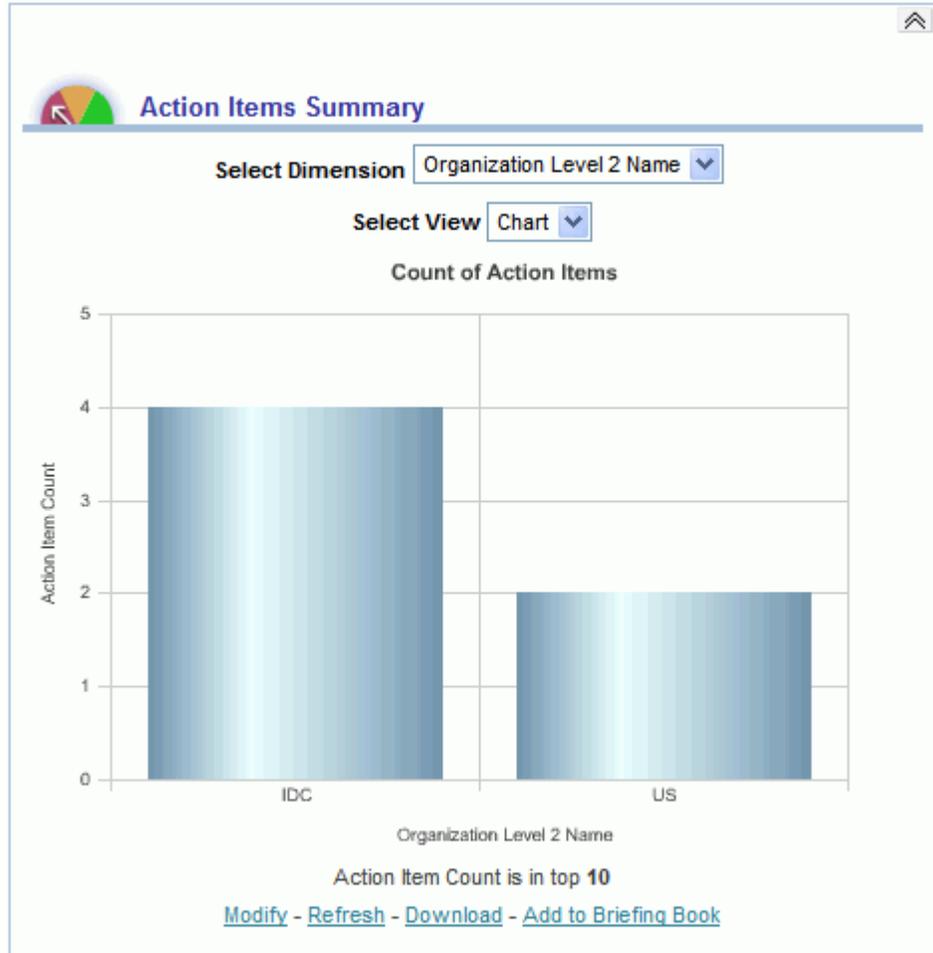
- **Action Items Details:** This landing report is for Action Items Summary. By clicking the Action Item Count count values, you can view the Action Items Detail report. The report displays the details of each action item, such as Title, Description, Status, Creation Date, Owner and Assigned To.

- **Design and Operating Effectiveness by Control:** Displays design and operating effectiveness by control. You can view this report as a table or as a chart.

Design and Operating Effectiveness by Control

Select View [Table ▼]

Control Type	In Scope	Control Title	Assessment Document ID	Assessment Type	Design Effectiveness	Design Failed %	Operating Effectiveness	Operating Failed %
Preventive	No	All Employees Receive Payment Vouchers	593	Operational,Design	Pass		Pass	
Preventive	No	New Control 1NA	578	Operational,Design	Pass			
Preventive	No	New Control 2NA	578	Operational,Design				
Preventive	No	Written policies and procedures, including a Revenue Recognition Policy	593	Operational,Design	Pass		Pass	
Preventive	No	Control1_sales	640	Operational,Design	Pass		Pass	

Records 1 - 5

Assessment Total Count is not null
and Control Key is not equal to / is not in -1

Modify - Refresh - Download - Add to Briefing Book

- **Assessment Status by Process Owner:** Displays the assessment status by process owner. Select a process in the Process Title column to view its details in GRC Manager.

Assessment Status By Process Owner

Select Dimension [Account Level 2 Name ▼]

Account Level 2 Name	Process Type	Process Document ID	Process Title	Process Owner	Assessment Due Date	Test Period	Assessment Title	Assessment Type	Assessment State	Completion Date
Payroll	Process	780	Payroll	icadmin		Y2008 Q4	RWS - Payroll	Operational	Owner Assessment	
Sales_Fin	Process	577	New Business Process 1NA	icadmin	10/1/2007	Y2012 Q4	Assessment - New Business Process 1NA	Operational,Design	Owner Assessment	10/1/2007
Sales_Fin	Process	636	Process_Sales	icadmin	10/24/2007	Y2012 Q4	Assessment - Process_Sales	Operational,Design	Completed	10/24/2007

Modify - Refresh - Download - Add to Briefing Book

- **Negative Reviewer Certification Responses by Process Owner:** Displays instances where an Executive Reviewer did not answer "Yes" to certify a process. Select the process owner's name to view details of their certification response.

Negative Reviewer Certification Responses By Process Owner
(Drill on Process Owner Name to view their Certification Responses)

| Process Owner	Process Type	Process Title	Reviewer	Reviewer Certification Question
icadmin	Process	New Business Process21	icadmin	I certify that the information in this assessment is accurate and complete to the best of my knowledge.

Reviewer Certification Answer Key is equal to _No

Modify - Refresh - Download - Add to Briefing Book

Certifications Dashboard

The Certification Dashboard consists of two tabs:

- Overview

- Activities
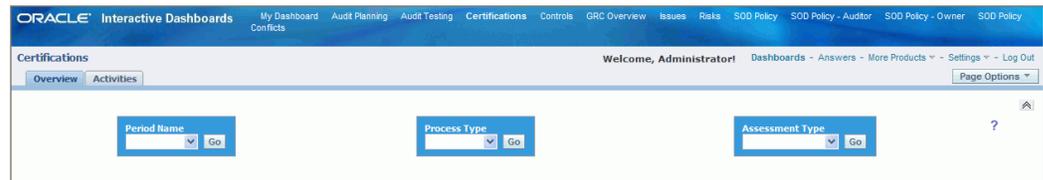
Certifications Overview Tab

The Certifications Overview tab consists of the following reports by default, but you can customize the page to add custom reports if desired. You can also choose to limit the reports by Period Name, Assessment Type and Process Type.

- **Certifications By Process - Current and Prior Year:** Shows Certifications by Process for the current and prior year. You can view this report as either a table or a chart. If you view it as a table, you can select a process in the Process Title column to view its details in GRC Manager. You can also select a year to view a breakdown by quarter.

  Note: The note you see on the report is due to a filter that was applied when the report shown in this example was created. The data within the filter is test data and is not applicable to your implementation. Refer to Appendix A of this guide for additional information on filters.

Certifications By Process - Current and Prior Year

Select Dimension: Account Level 2 Name

Select View: Table

Year	Account Level 2 Name	Process Document ID	Process Title	Certified Count	Year Ago Certified Count (Completion Date)
2008	Accounting	11	Process1_0320	1	
2008	Accounting	46	Process_HQsales	0	
2008	Accounting	64	Process_Issues	0	
2008	Accounting	158	Process4_0320	1	

Certified Count is not null

and Process Key is not equal to / is not in **0**

and Process Type is equal to **Process**

Modify - Refresh - Download - Add to Briefing Book

- **Design and Operating Effectiveness by Process:** Displays design and operating effectiveness by process. If you choose to display this report as a chart, you can click on a column to see a further breakdown of the failure by process. If you display it as a table, you can select a process in the Process Title column to view its details in GRC Manager.
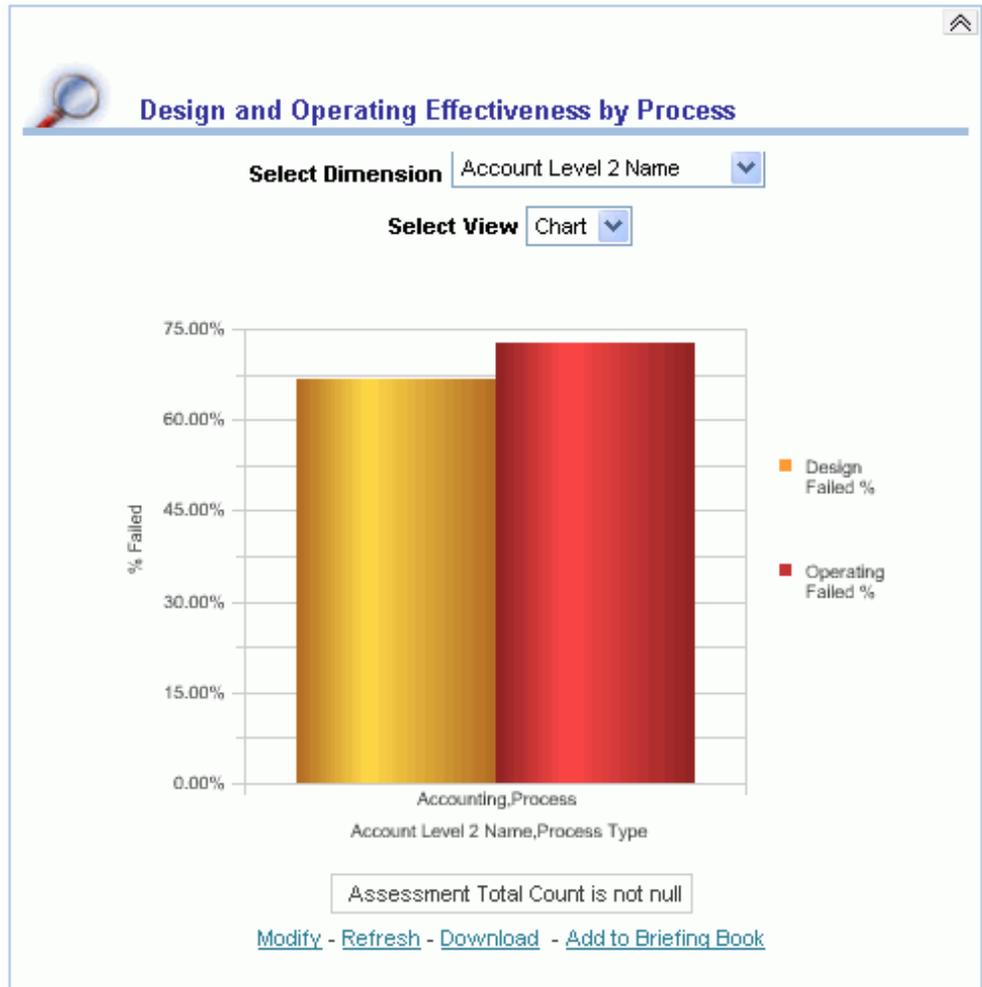
- **Open Assessments by Due Date:** Displays the days by which an assessment is overdue for completion. A negative value that displays in red signifies that the assessment is due after the number of days specified. A positive value in black signifies that the due date has passed by the specified number of days. You can drill to GRC Manager by selecting a process or assessment title.

  In tables, underlined links lead to external data, and plain links stay within GRCI. For example, in this table, the underlined links invoke GRC Manager to show details of the process and assessments.

  > **Note:** Please be aware that sometimes the Process Doc ID in not underlined and it is a hyperlink to GRCM, which enables you to view the process document.

Certifications Activities Tab

The Certifications Activities tab consists of the following reports by default, but you can customize the page to add custom reports if desired. You can also choose to limit the reports by Period Name, Control Type, Assessment Type, and Process Type using the dashboard prompts.

- **Assessment Status By Process Owner:** Displays the assessment status by process owner. Select a process in the Process Title column to view its details in GRC Manager.
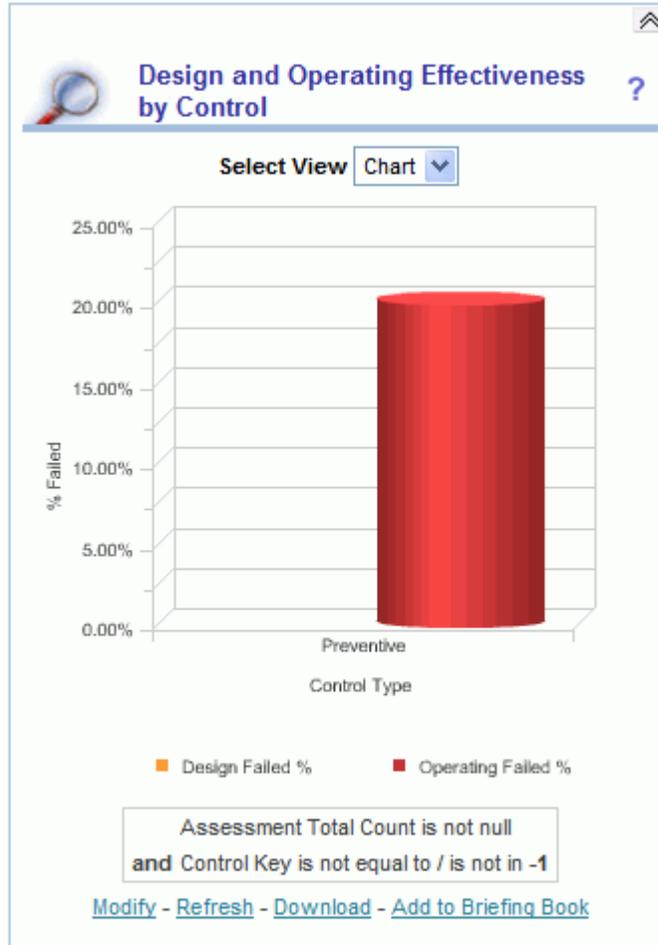

- **Design and Operating Effectiveness by Control Report:** Displays design and operating effectiveness by control. You can view this report as a table or as a chart.

- **Negative Reviewer Certification Responses By Process Owner:** Displays instances where an Executive Reviewer did not answer "Yes" to certify a process. Select the process owner's name to view details of their certification response.

Controls Dashboard

The Controls Dashboard consists of two tabs:

- Overview

- Activities

Controls Overview Tab

The Controls Overview tab consists of the following reports by default, but you can customize the page to add custom reports if desired. You can also choose to limit the reports by Period Name, Control Type, and Process Type using the dashboard prompts.

- **Controls Summary:** Displays the count of control tests by control and account type, with the percentage of passed and failed control tests. Select a control title to display details of the control in GRC Manager.

  Note: The note you see on the report is due to a filter that was applied when the report shown in this example was created. The data within the filter is test data and is not applicable to your implementation. Refer to Appendix A of this guide for additional information on filters.

- **Processes With Control Issues:** Displays processes with control issues. Select a process title to display details of the process in GRC Manager, or select a Process Document ID to view additional details.

- **Processes With Control Issues - Details:** This is a landing report for Processes with Control Issues. This report has issues information such as issue status, severity, and issue count details for process and associated controls.

- **Accounts Lacking Mitigating Controls:** Displays accounts that do not have subordinate or monitoring controls.

- In the Key control column, Red highlighting indicates that there are no key controls, which is a problem that must be addressed.

- In the Subordinate control column, yellow highlighting indicates that there are no mitigating controls and you should perform follow up to ensure that is appropriate.

- **Controls Account - Key Control:** This landing report is for Accounts Lacking Mitigating Controls. In the parent report when you click the Key Control Count value, you will open the Controls Account - Key Control report. The Controls Account - Key Control report is a detail level drill down report which contains the control information along with their Key Control count.

- **Manual versus Automated Control and Risk Rating Comparison:** Summarizes the number of control issues by control type and method. Green highlighting with a flag indicates that there are no control issues.

- **Control Test Summary:** Displays by process and control type the total count of control tests and the percentage of tests that are Open and Closed. In the Closed Test column:

  - Red highlighting indicates 0-50% of the tests are closed

  - Yellow highlighting indicates that between 51-84% of the tests are closed

  - Green indicates that 100% of the tests are complete

- **Assertion Control Test Summary:** Displays Control Test Results by selected Dimension, Process, and Assertion.
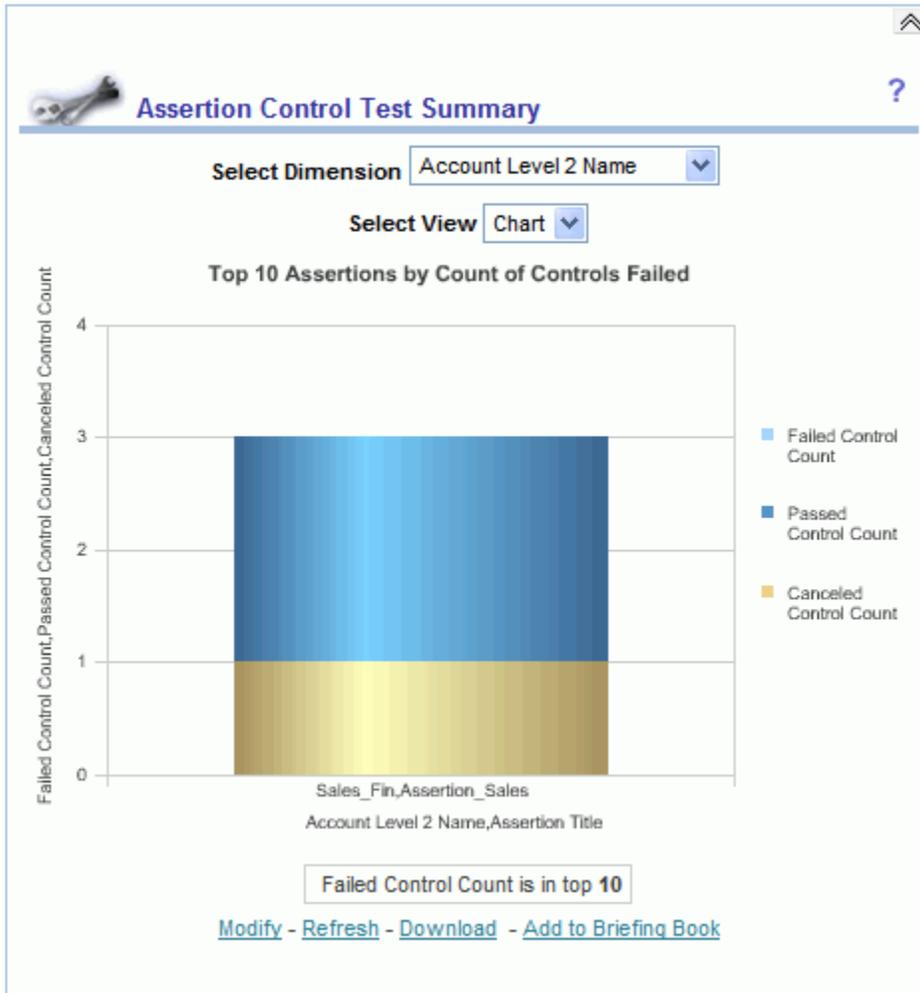
- **Assertion Control Test Fail - Detail:** This is a landing report for Assertion Control Test Summary, from the Table view select a Failed Control Count value. This report shows test result with failed status and related assertion and control details of that completed test.

- **Assertion Control Test Pass - Detail:** This is also a landing report for Assertion Control Test Summary. This report shows test results with passed status and related assertion and control details of that completed test.

- **Assertion Control Test Cancelled - Detail:** This is a landing report for Assertion Control Test Summary. This report shows test result with cancelled status and related assertion and control details of that completed test.

Controls Activities Tab

The Control Activities tab consists of the following reports by default, but you can customize the page to add custom reports if desired. You can also choose to limit the reports by Period Name, Control Type, and Process Type using the dashboard prompts.

- **Controls Count - Summary:** Displays the number of Key Controls for each process. You can select a different dimension or metric by which to view the report. Select a dimension value, Process Type or Process Document ID to view details in GRC Intelligence; select a Process Title to view details in GRC Manager.

Controls Count - Summary

Select Dimension	Account Level 2 Name		Select Metric	Key Control Count	

Account Level 2 Name	Process Type	In Scope	Process Title	Process Document ID	Key Control Count
Fin Node 01	Policy	No	New Business Process31	56	0
Fin Node 01	Policy	Yes	BP01	82	0
Fin Node 01	Policy	Yes	BP01	133	0
Fin Node 01	Policy	Yes	BP bug 7608954	121	0
Fin Node 01	Policy	No	New Business ProcessYGO	159	0

Records 1 - 5

Modify - Refresh - Download - Add to Briefing Book

- **Number of Controls Failures By Risk Type:** Displays the number of control failures by risk type for an organization. Select Table View to drill on a Risk Type to view Control Failures by Process report.

- **Controls Test Failures:** Displays by test period and test owner, the status and results of completed tests. Select a Control Title to view its details in GRC Manager.

- **Control Failure By Process:** Displays control failures by process for an organization. Select a process title to view its details in GRC Manager, or drill on a Failed Control Count value to see the Control Detail Account report.

Issues Dashboard

The Issues Dashboard consists of two tabs:

• Overview

• Activities
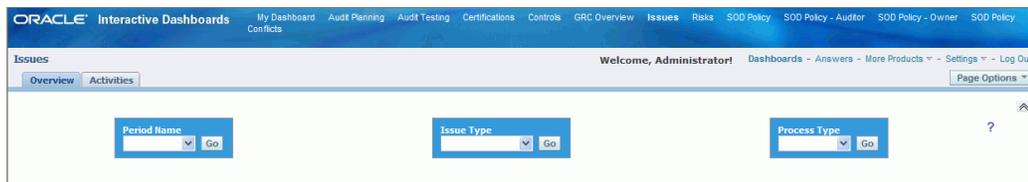
Issues Overview Tab

The Issues Overview tab consists of the following reports by default, but you can customize the page to add custom reports if desired. You can also choose to limit the reports by Period Name, Issue Type, and Process Type using the dashboard prompts.

- **Issues - Deficiencies Summary:** Displays a summary of Issues-deficiences. Select a value to see detail information, or select an Issue Title to see the issue in GRC Manager.

Issues - Deficiencies Summary
(Drill on value to see detail information)

Select Dimension: Organization Level 2 Name

Organization Level 2 Name	Issue Type	Material Weakness Count	Significant Deficiency Count	Deficiency Count	Documentation Count
CSprings	Assessment	2	0	0	0
CSprings	Control Evaluation	1	1	0	0
CSprings	Evaluation	1	1	2	0
CSprings	Process	1	3	4	3
HQ_Sales	Assessment	1	0	1	2

Records 1 - 5

Modify – Refresh – Download – Add to Briefing Book

- **Audit and Process Test Issues:** Displays the number of issues that exist for Audit and Process Tests. Select a value to see detail information, or select a Process Title to see the Process and its related issues in GRC Manager.

Audit and Process Test Issues
(Drill on values to see detail information)

Select Dimension: Organization Level 2 Name

Organization Level 2 Name	Issue Type	Process Type	In Scope	Process Title	Process Document Name	Process Document ID	Process Test Issue Count	Audit Test Issue Count
IDC	Assessment	Policy	Yes	BP bug 7608954	000100	121	0	0
IDC	Assessment	Policy	No	New Business ProcessYGO	000131	159	0	0
IDC	Control Evaluation	Policy	No	New Business Process31	000031	56	0	1
IDC	Control Evaluation	Policy	Yes	BP01	000069	133	0	1
IDC	Evaluation	Policy	No	New Business ProcessYGO	000131	159	6	0

Records 1 - 5

Modify - Refresh - Download - Add to Briefing Book

- **Issues Scorecard Summary:** Displays a count of Risk, Control, Assertion, and Process Issues. Select a value to see detail information.

Issues Scorecard Summary
(Drill on values to see more detail information)

?

Select Dimension: Organization Level 2 Name ▼

Organization Level 2 Name	Issue Type	Issue State	Risk Issue Count	Control Issue Count	Process Issue Count	Assertion Issue Count
CSprings	Assessment	Hold	0	0	0	0
CSprings	Assessment	Open	0	0	0	0
CSprings	Control Evaluation	Open	0	2	0	0
CSprings	Evaluation	Closed	0	0	0	0
CSprings	Evaluation	Edit	0	0	1	0
CSprings	Evaluation	Open	0	1	0	1
CSprings	Process	Closed	0	0	0	0
CSprings	Process	Open	1	0	2	5
HQ_Sales	Assessment	Closed	0	2	0	0
HQ_Sales	Assessment	Open	1	0	1	1

◁◁ ◁   ▷ ▷* Records 1 - 10

Modify – Refresh – Download – Add to Briefing Book

- **Processes With Risk and Control Issues:** Displays Processes with risk and control issues. Select a value to see detail information, or select a Process Title to see the Process and its related issues in GRC Manager.

- **Processes Assertion Issue Summary:** Displays the number of issues associated assertions. This includes:

  - Dimension

  - Process Title

  - Assertion Issue

  - Issue Type

  - Issue Title

  - Issue State

  - Deficiency

  - Owner
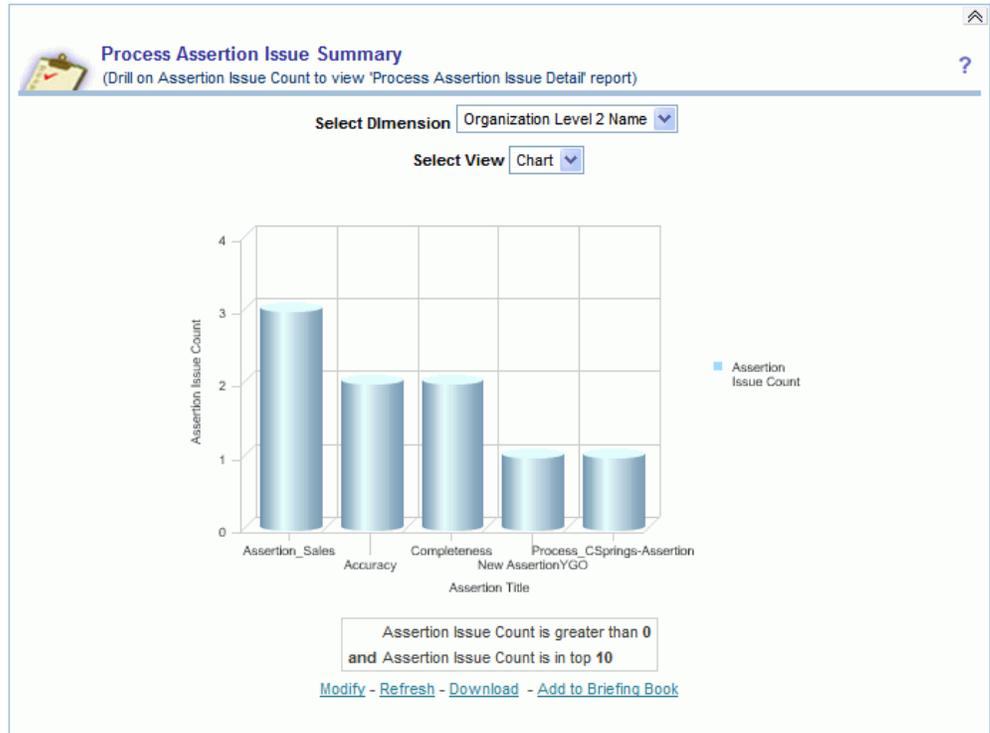
Issues Activities Tab

The Issues Activities tab consists of the following reports by default, but you can customize the page to add custom reports if desired. You can also choose to limit the reports by Period Name and Issue Type using the dashboard prompts.

- **Issues Requiring Remediation:** Displays issues that require remediation. You can limit this report by dimension, and you can view this report as chart or table. If you choose to view it as a table, you can select an Issue Title to view the details of that issue in GRC Manager.

- **Issues by Materiality:** Displays issues by materiality. You can limit this report by dimension or metric, and you can view this report as chart or table. If you choose to view it as a table, you can select an Issue title to view the details of that issue in GRC Manager.
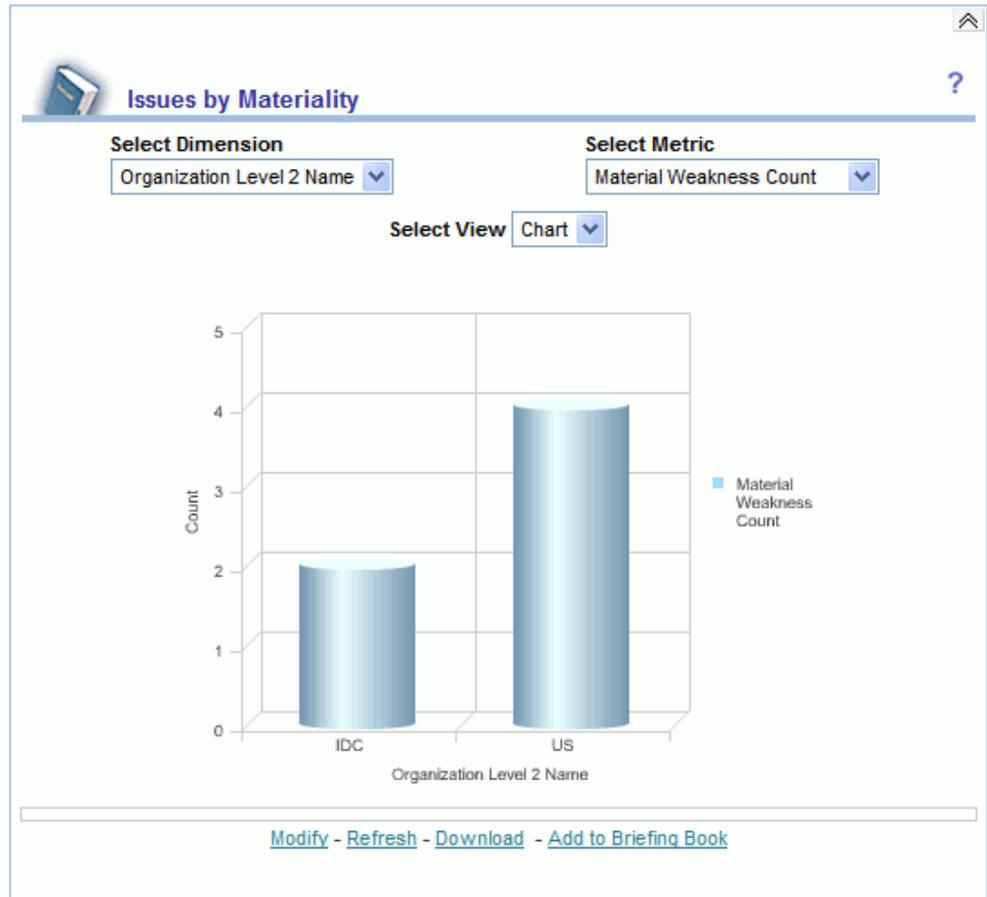
- **Issues Trends:** Displays Process Issue, Audit Test Issue, Assessment Issue, and Process Test Issue Counts over time.
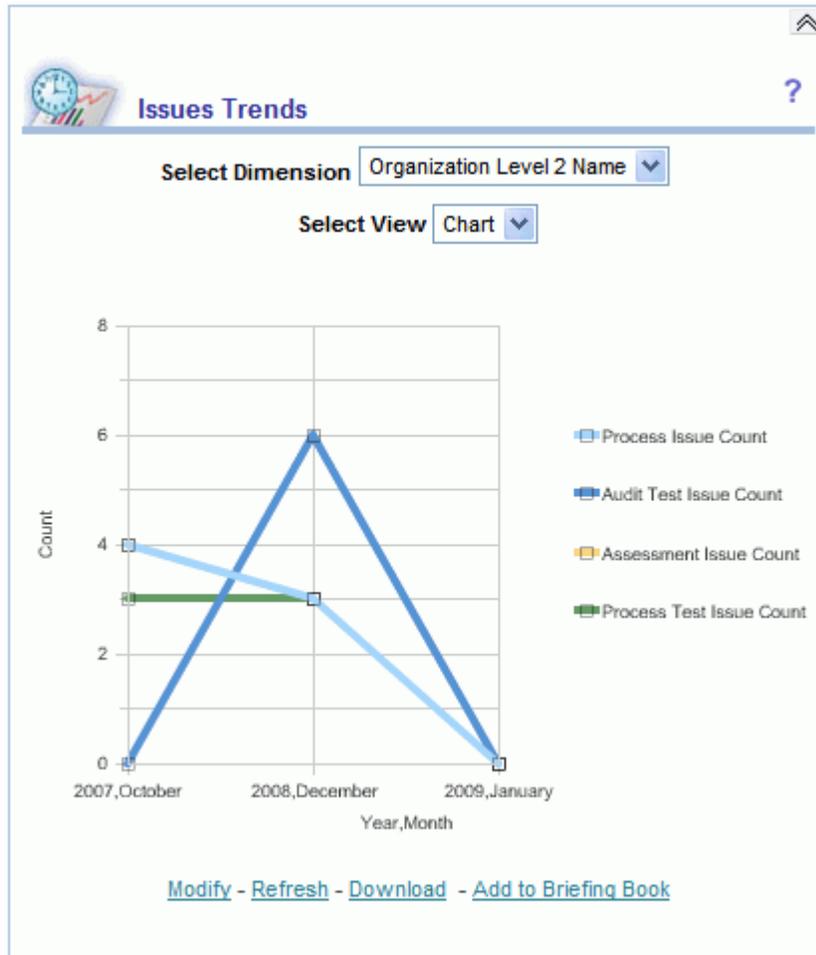
- **Issues By Originator:** This report shows issue details and days past due by Issues Originator.

Risks Dashboard

The Risk Dashboard consists of two tabs:

• Overview

• Activities

Risks Overview Tab

The Risk Overview tab consists of the following reports by default, but you can customize the page to add custom reports if desired. You can also choose to limit the reports by Period Name, Risk Type, Control Type, and Process Type using the dashboard prompts.

• **Risk Mitigation By Risk and Process Type:** Displays risk mitigation by process and risk type. In Chart view, select a Process Type or a Risk Type to view details. In Table view, select a key or subordinate count to view the Controls Account report.

Risk Mitigation By Risk and Process Type

(Drill on Key or Subordinate Count to view detail Controls Account report)

Select Dimension: Account Level 2 Name   Select Type: Risk Type
Select View: Table

Account Level 2 Name	Process Type	In Scope	Control Type	Control Method	Risk Type	Process Count	Key Control Count	Key Control Count %	Subordinate Control Count	Subordinate Control Count %
Fin Node 01	Policy	No	Corrective	Auto Monitoring	Regulatory Compliance	2	0	0.00%	0	0.00%
		Yes		Auto Monitoring	Theft of Services	2	0	0.00%	0	0.00%
		No		Automated	Theft of Assets	1	0	0.00%	0	0.00%
		Yes		Control Automation	Regulatory Compliance	1	0	0.00%	0	0.00%
		No	Detective	Auto Monitoring	Regulatory Compliance	1	0	0.00%	0	0.00%
	Process	Yes	Corrective	Auto Monitoring	Regulatory Compliance	1	0	0.00%	0	0.00%
		No		Auto Monitoring	Regulatory Compliance	1	0	0.00%	1	50.00%
		No	Detective	Automated	Theft of Services	3	0	0.00%	0	0.00%
		No		Manual	Theft of Assets	2	2	100.00%	0	0.00%
		No	Preventive	Control Automation	Regulatory Compliance	1	0	0.00%	1	50.00%
		No		Manual	Theft of Services	3	0	0.00%	0	0.00%

Modify - Refresh - Download - Add to Briefing Book

- **Controls Account - Key Control:** This is a detail level drill down report which contains control information along with key control count information.

Risks

Controls Account - Key Control

Control Document ID	Control Title	Control Type	In Scope	Key Control Count
23	New Control 01	Detective	No	2

Return - Modify - Refresh - Download - Add to Briefing Book - Create Bookmark Link

- **Controls Account - Subordinate Control:** This is a detail level drill down report which contains control information along with subordinate control count information.

- **Number of Controls Failures By Risk Type:** Displays the count of control tests, and failed control counts by risk type, for an organization. In the table view, select a Risk Type to view Control Detail Account - Failures Control Count.
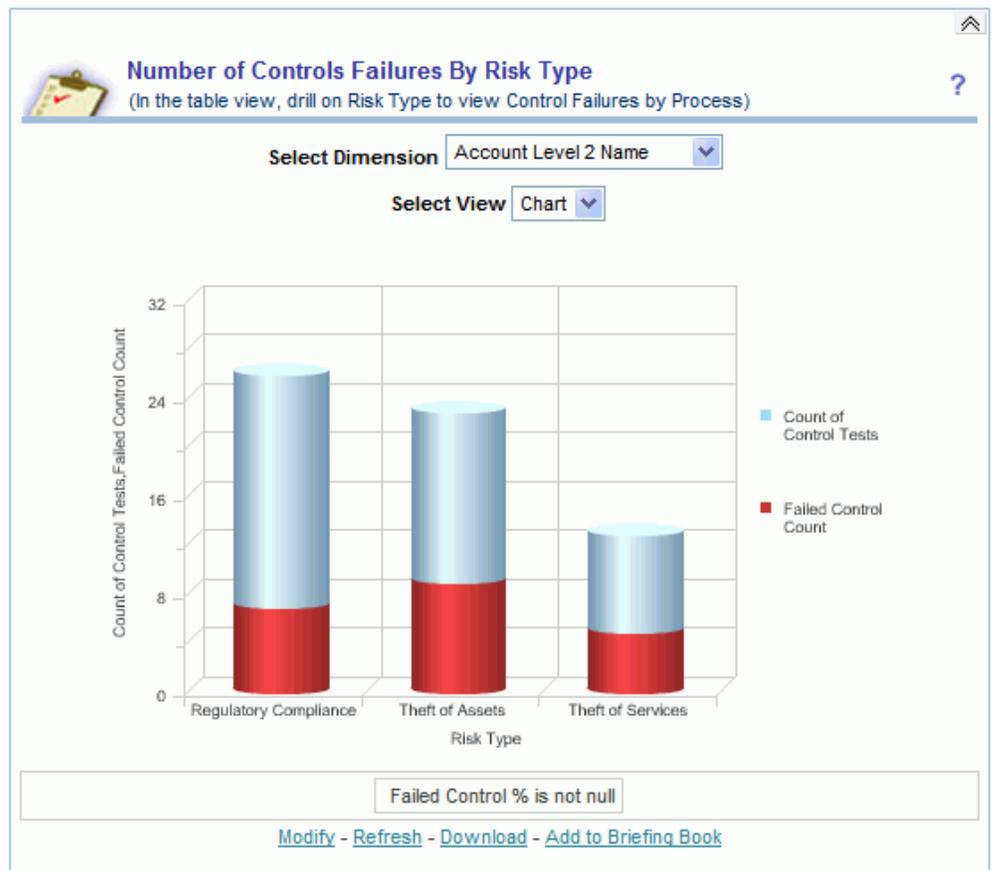
- **Control Detail Account - Failures Control Count:** This is a detail level drill down report which contains control information along with failed control count test information.

Risks

Control Detail Account - **Failed Control Count**

Control Document ID	Control Title	In Scope	Control Type	Failed Control Count
87	Control 01	No	Corrective	1
88	Control 02	Yes	Corrective	3
118	BP bug 7608954	Yes	Corrective	1

Return – Modify – Refresh – Download – Add to Briefing Book – Create Bookmark Link

- **Manual versus Automated Control and Risk Rating Comparison:** Displays manual versus automated controls and risk comparisons. Select a Control Method to view details.

Manual versus Automated Control and Risk Rating Comparison

Select Dimension Organization Level 2 Name

Organization Level 2 Name	Control Type	In Scope	Control Method	Risk Rating	Control Issue Count
CSprings	Detective	No	Auto Monitoring	6	
CSprings	Preventive	No	Manual	6	3
HQ_Sales	Preventive	No	Automated	2	1
HQ_Sales	Preventive	No	Manual	7	7
Sales_org	Preventive	No	Manual	4	

Modify – Refresh – Download – Add to Briefing Book

- **High Risk Processes:** Displays details of the Key Control Counts and Risk Type associated with a given process (e.g. risk rating, risk significance, risk likelihood, and risk type).

- **Risks by Process - Issues Aging:** Displays issues that relate to high risk processes, as well as open issues that are aging and in overdue status. Select a risk title to view details of the risk in GRC Manager.

Risks Activities Tab

The Risk Activities tab consists of the following reports by default, but you can customize the page to add custom reports if desired. You can also choose to limit the reports by Period Name, Risk Type, and Process Type using the dashboard prompts.

- **High Risk Processes With Issues:** Displays high risk processes with issues. Select a count to view details for the selected issues.

High Risk Processes With Issues

Select Dimension: Organization Level 2 Name
Select View: Chart
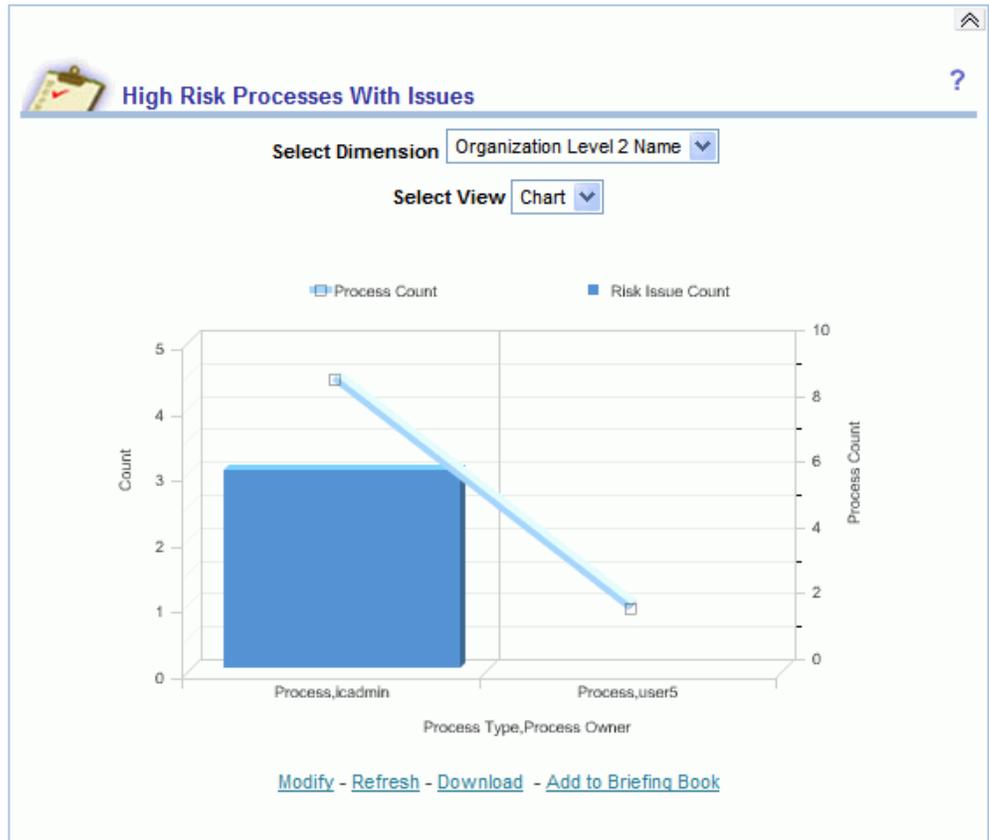
- **Risk by Process Owners:** Displays average risk processes by process owner. In the table view, select a Process Title to view details of the process in GRC Manager.
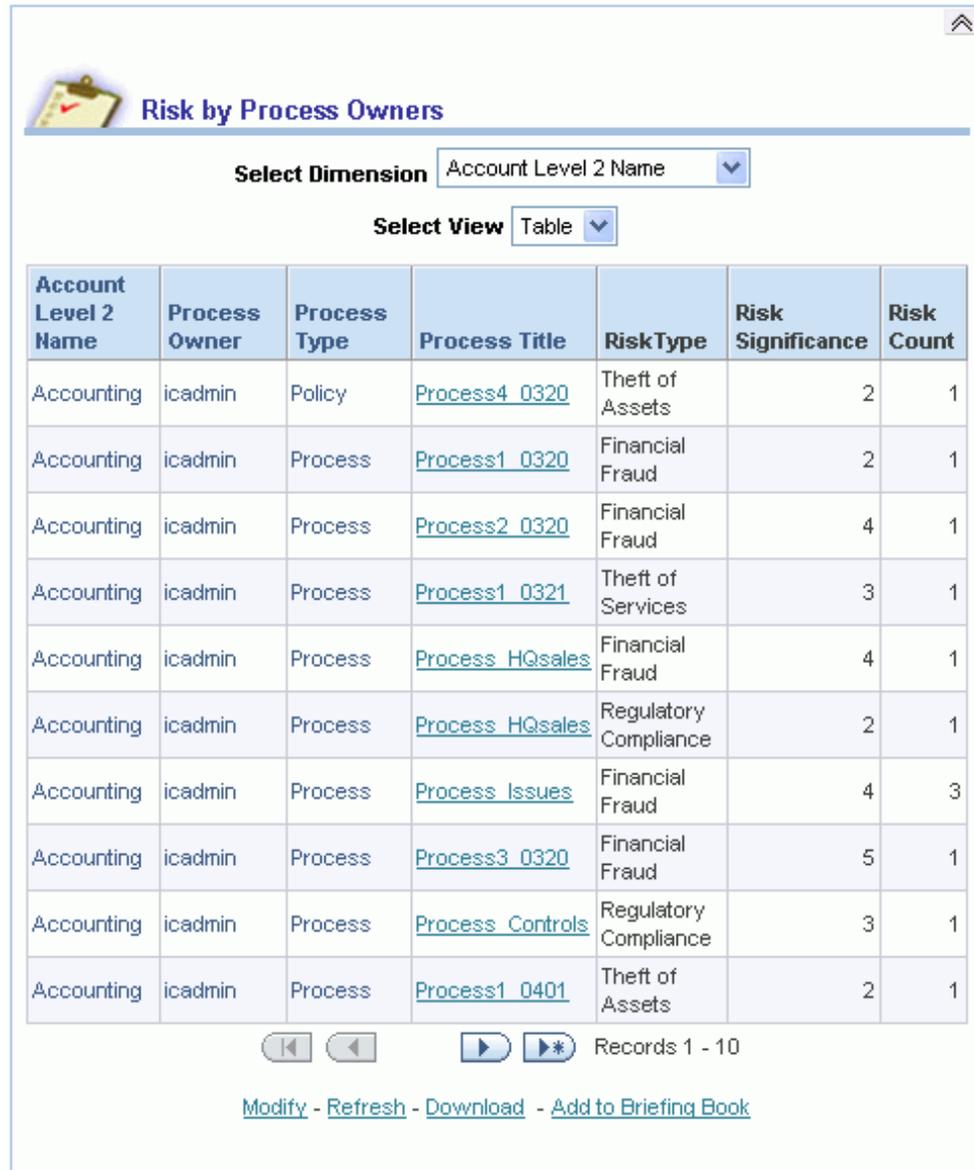
Risk by Process Owners

Select Dimension Account Level 2 Name

Select View Table

Account Level 2 Name	Process Owner	Process Type	Process Title	RiskType	Risk Significance	Risk Count
Accounting	icadmin	Policy	Process4_0320	Theft of Assets	2	1
Accounting	icadmin	Process	Process1_0320	Financial Fraud	2	1
Accounting	icadmin	Process	Process2_0320	Financial Fraud	4	1
Accounting	icadmin	Process	Process1_0321	Theft of Services	3	1
Accounting	icadmin	Process	Process_HQsales	Financial Fraud	4	1
Accounting	icadmin	Process	Process_HQsales	Regulatory Compliance	2	1
Accounting	icadmin	Process	Process_Issues	Financial Fraud	4	3
Accounting	icadmin	Process	Process3_0320	Financial Fraud	5	1
Accounting	icadmin	Process	Process_Controls	Regulatory Compliance	3	1
Accounting	icadmin	Process	Process1_0401	Theft of Assets	2	1

Records 1 - 10

Modify - Refresh - Download - Add to Briefing Book

- **Number of Controls By Risk Type and Significance:** Displays the number of controls by risk significance and preventative control counts based on Risk Type. Select a Preventative Control Count to view the Controls Account - Preventive Control Count report.
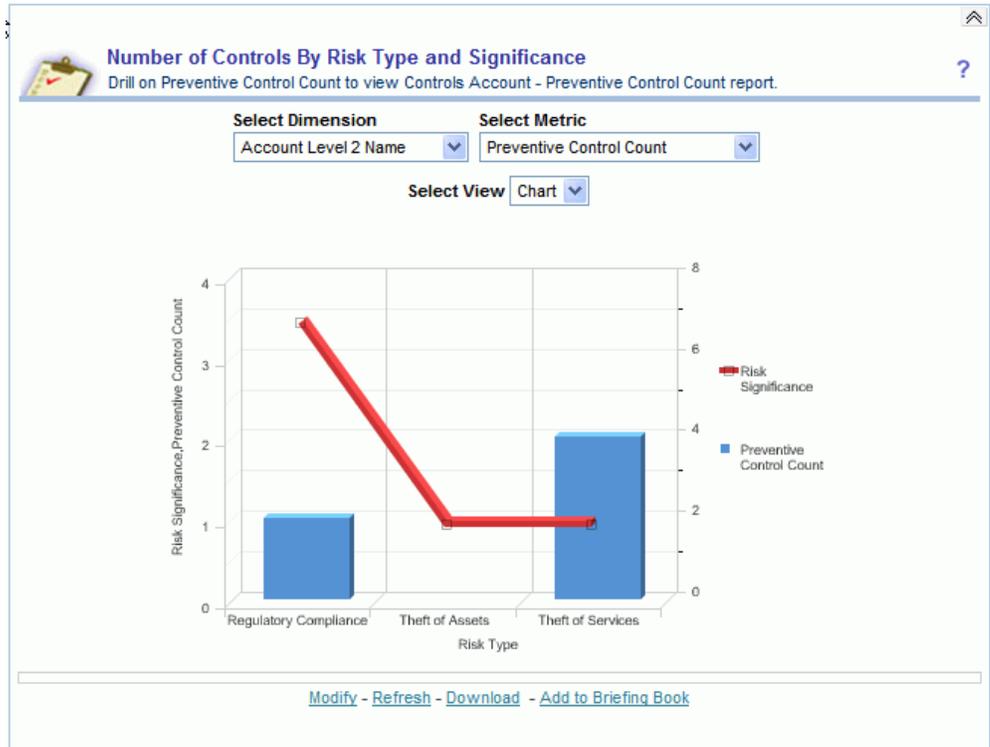
- **High Risk Processes With No Controls Tested:** Displays high risk processes with no controls tested, and the count of the risks. Select a Process Title to view details of the process in GRC Manager. The Control Count column was added.

- **Assertion Risk Control Matrix:** This report displays information about the assertion, risks, and controls for a process and the relationship between them.

> **Important:** It does not include processes in a Retired state.
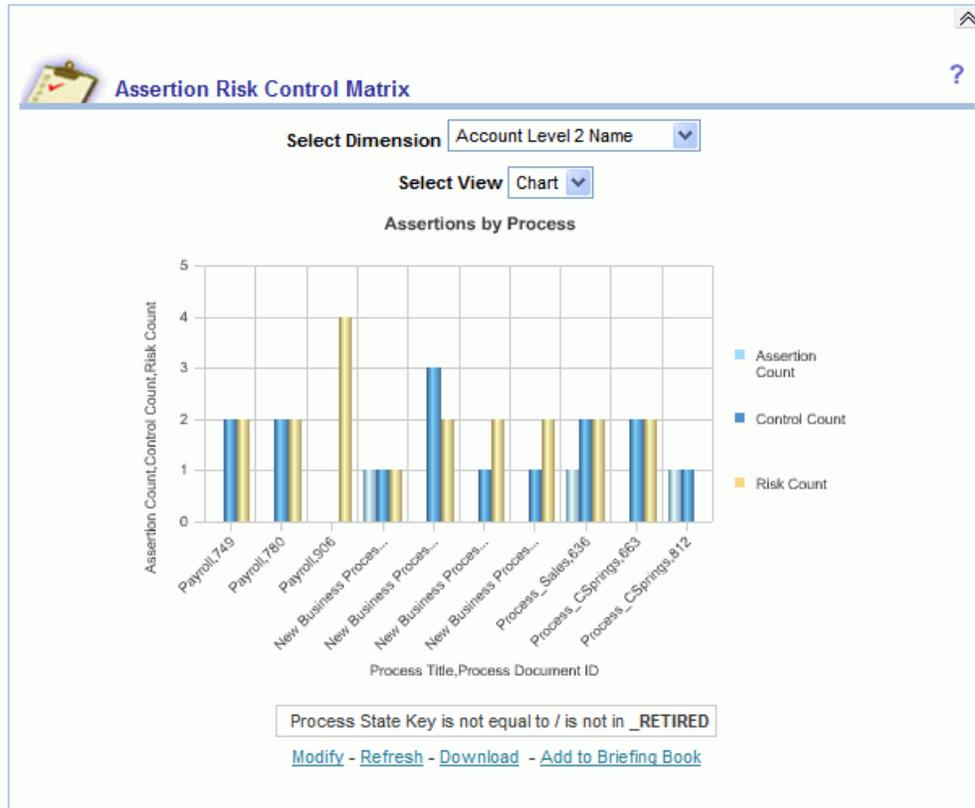
- **Strategic Risk Analysis:** This report displays a filter to represent the Assertions based on Risk Criticality and Assertion State Key.
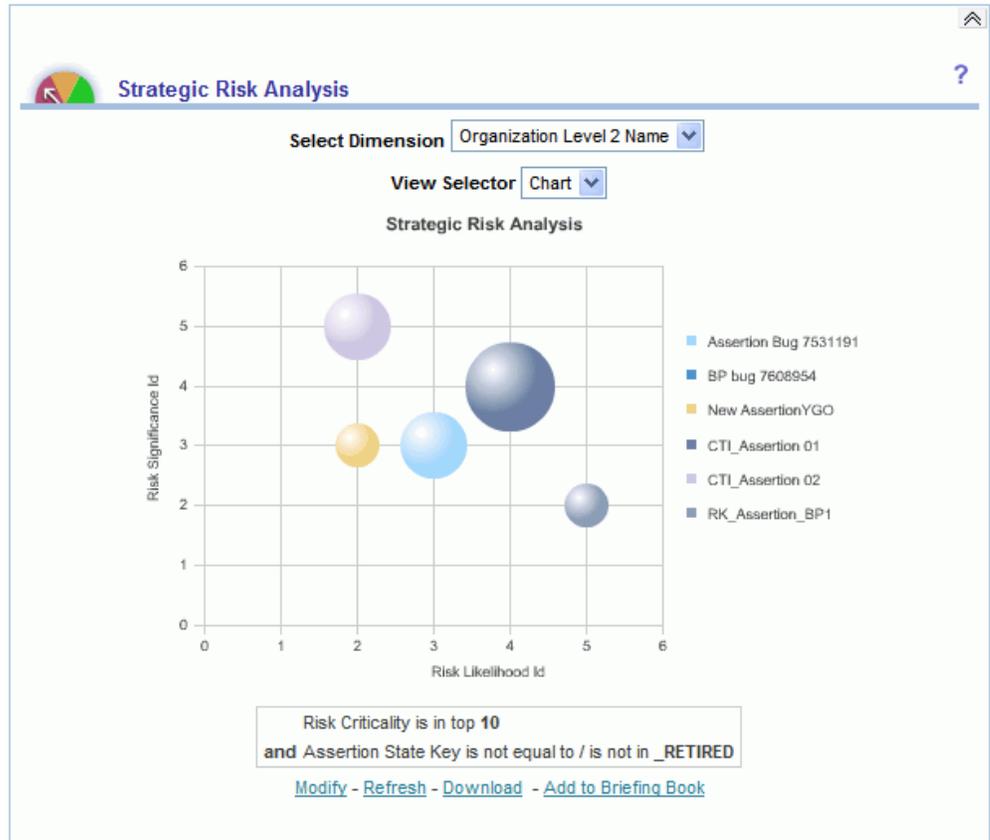
Audit Testing Dashboard

The Audit Testing Dashboard consists of two tabs:

- Overview

- Activities

On either Audit Testing Dashboard tab, you can choose to limit the reports by using the following prompts:

- Period Name

- Control Type

- Process Type

Audit Testing Overview Tab

The Audit Testing Overview tab consists of the following reports by default, but you can customize the page to add custom reports if desired. You can also choose to limit the reports by Period Name, Control Type, and Process Type.

- **Control Test Summary:** Displays a summary of tests based on test type and process detailing the total number of tests and the percentage of those tests that are open or closed. Select a Process Title to view details of the process in GRC Manager.

If, for example, you were to select Process2_0320, you would see the following screen in GRC Manager:

- **Test Coverage - Current and Prior Year:** Displays test coverage by organization for the current and prior year. In Table view, select a Process Title to view details of the process in GRC Manager. In this example, the account is new, so there is no data available for the prior year, and thus those columns are empty.

Test Coverage - Current and Prior Year: Table View

Year	Account Level 2 Name	Process Type	Process Title	Control Document ID	In Scope	Count of Control Tests	Year Ago Total Test Count	Year Ago Open Count	Current Flag	Current Flag Key
2008	Fin Node 01	Policy	New Business Process31	51	No	2	0	0	Current	_Current
		Process	New Business Process 01	23	No	2	0	0	Current	_Current
2009	Fin Node 01	Policy	New Business Process31	51	No	1	0	0	Current	_Current
						1	0	0	Current	_Current
			BP01	87	No	1	0	0	Current	_Current
						2	0	0	Current	_Current
				88	Yes	4	0	0	Current	_Current
			BP bug 7608954	118	Yes	1	0	0	Current	_Current
						2	0	0	Current	_Current
			New Business ProcessYGO	155	No	1	0	0	Current	_Current
						4	0	0	Current	_Current
						1	0	0	Current	_Current
		Process				2	0	0	Current	_Current
			New Business Process 01	23	No	1	0	0	Current	_Current
						2	0	0	Current	_Current
						1	0	0	Current	_Current
			New Business Process21	170	No	2	0	0	Current	_Current
						1	0	0	Current	_Current
			Bug 7531191	95	Yes	2	0	0	Current	_Current
						1	0	0	Current	_Current
			RK_BP1	187	No	1	0	0	Current	_Current
				188	No	1	0	0	Current	_Current

Current Flag Key is equal to _Current

Modify – Refresh – Download – Add to Briefing Book

Test Coverage - Current and Prior Year: Chart View

- **Audit and Process Test Issues:** Displays audit and process test issues. Select a value to see detail information.

- **Issue Scorecard Detail - Process Test Issues:** This is a landing report for Audit and Process Test Issues. In the Audit and Process Test Issues report when you click the Process Test Issue Count value this will lead to the Issues Scorecard Detail - Process Test Issues report.

- **Issue Scorecard Detail - Audit Test Issues:** This is also a landing report for Audit and Process Test Issues. In the Audit and Process Test Issues report when you click the Audit Test Issue Count value it takes you to the Issues Scorecard Detail - Process Test Issues report.

- **Open Assessments by Due Date:** Displays the number of days by which an assessment is overdue for completion. Select a Process Title or an Assessment Title to view details in GRC Manager.

- **Assertion Control Test Summary:** This report displays information about Assertions, Controls and the Control Status by test result.
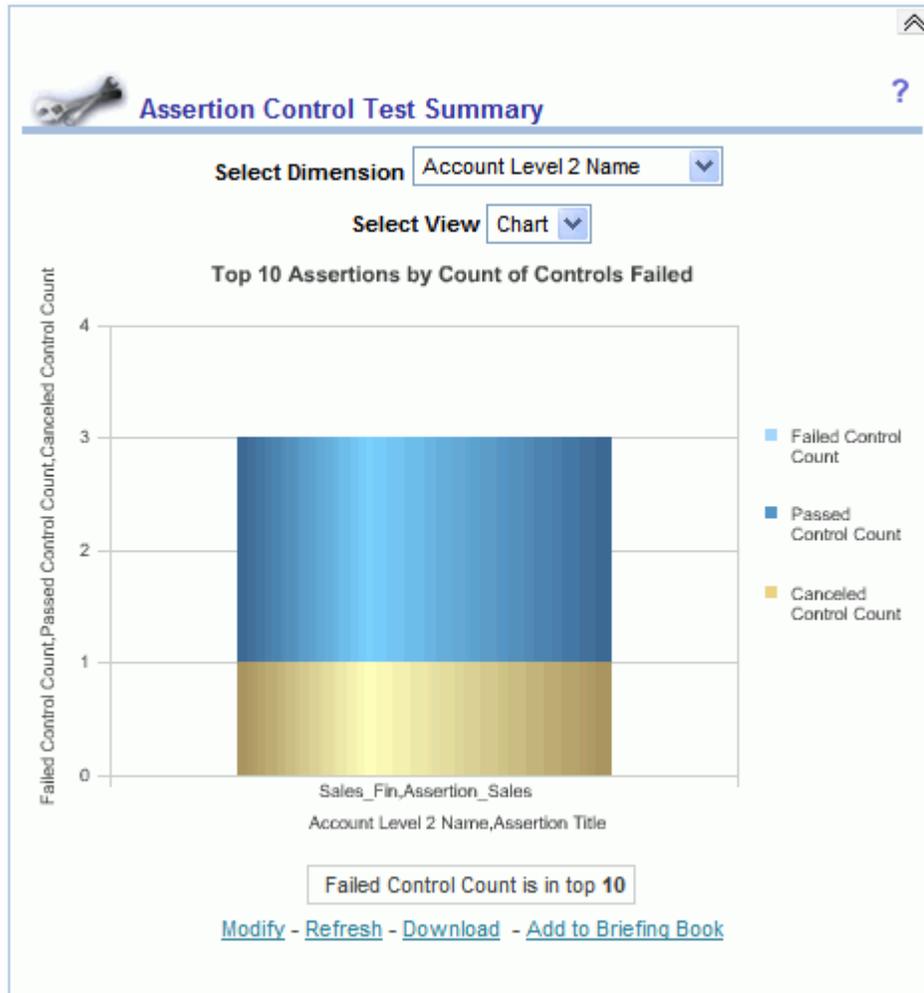
Audit Testing Activities Tab

The Audit Testing Activities tab consists of the following reports by default, but you can customize the page to add custom reports if desired. You can also choose to limit the reports by Period Name, Control Test Type, and Process Type using the dashboard prompts.

- **Testing Cycle Time - Test Owner:** Displays the testing cycle time, in elapsed days, by test owner.

- **Controls Test Failures:** Displays, by test period and test owner, the status and results of completed tests. Select a Control Title to view its details in GRC Manager.

- **Tests Completed By Test Owner - Current and Prior Year:** Displays tests completed for the current and prior year by test owner. In Chart view, select a test count to view details. In Table view, select a Process title to view its details in GRC Manager.
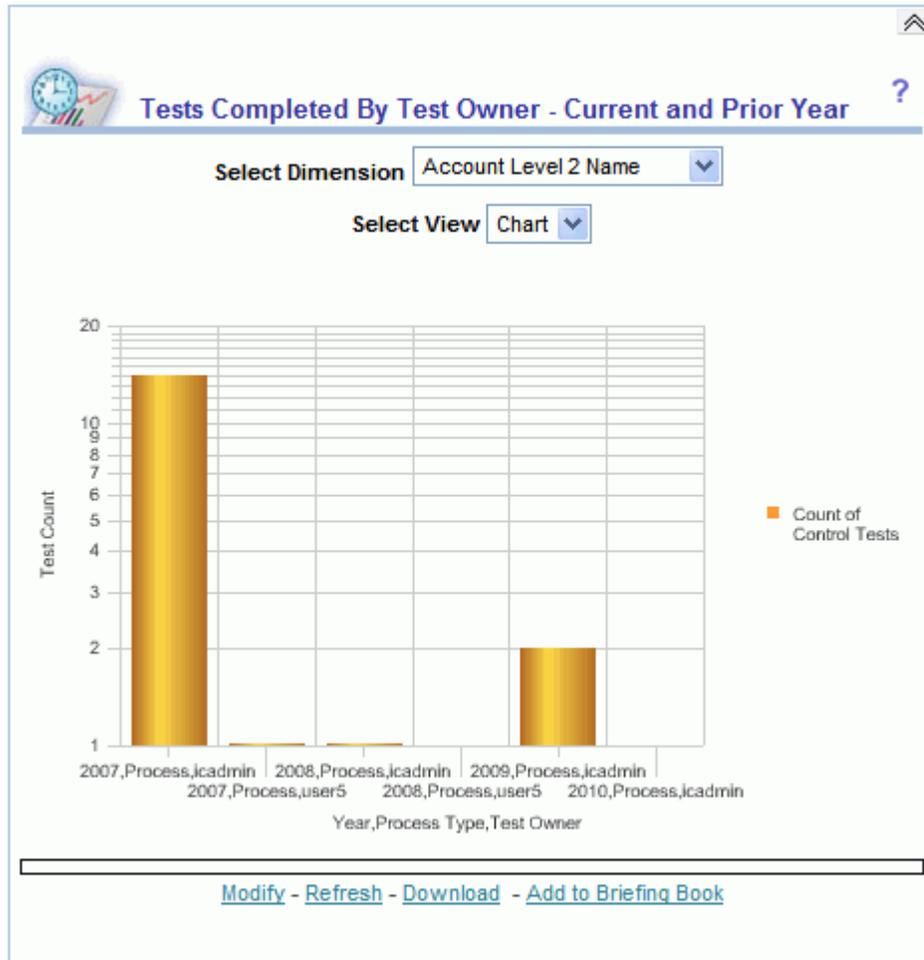
Audit Planning Dashboard

The Audit Planning Dashboard consists of two tabs:

- Overview

- Activities
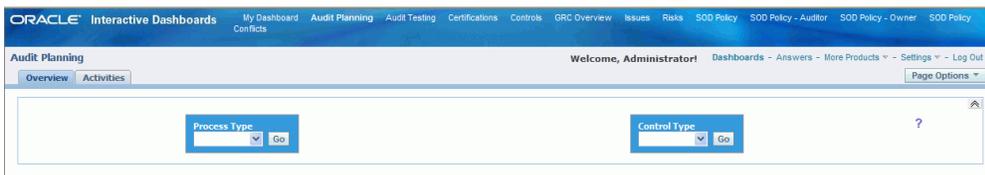
Audit Planning Overview Tab

The Audit Planning Overview tab consists of the following reports by default, but you can customize the page to add custom reports if desired. You can choose to limit the reports by selecting a Process Type or Control Type prompt. You can also use the following report filters: Test Plan Title, Process Title, and Assertion Title.

- **Audit Test Plan Summary: Table View and Chart View** Use this report to view Audit Test Plans, Assertions, and Controls to be tested.

- **Controls not included in Test Plans - Details:**This report identifies and displays all Controls currently not included in Audit Test Plan.

Controls not included in Test Plans - Detail

Select View Chart

Controls Not Included in Audit Test Plans
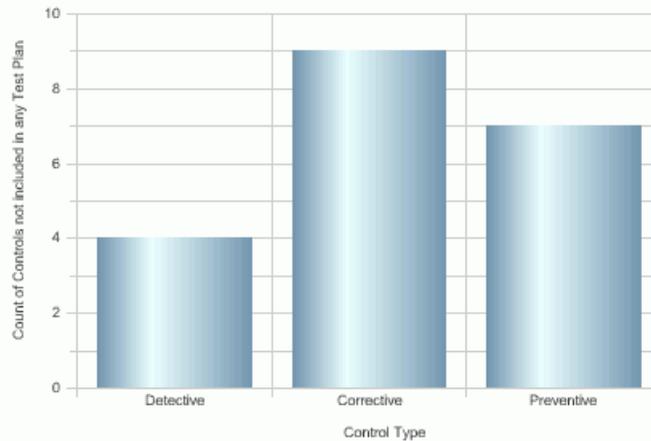
Control Count – CASE WHEN Test Plan Control Count IS NULL THEN 0 ELSE Test Plan Control Count END is greater than **0** and Process Document ID is not equal to / is not in **-1**

- **Control Test Instruction Summary:**This report enables the user to view all controls related to an Organization, Process or Risk, by Type, with Count of Test Instructions, details of related Audit Plans, and Count of Canceled Test results.

1. The X-axis contains the "Process Title".

2. The Y-axis shows only one measure, "Count of Controls".
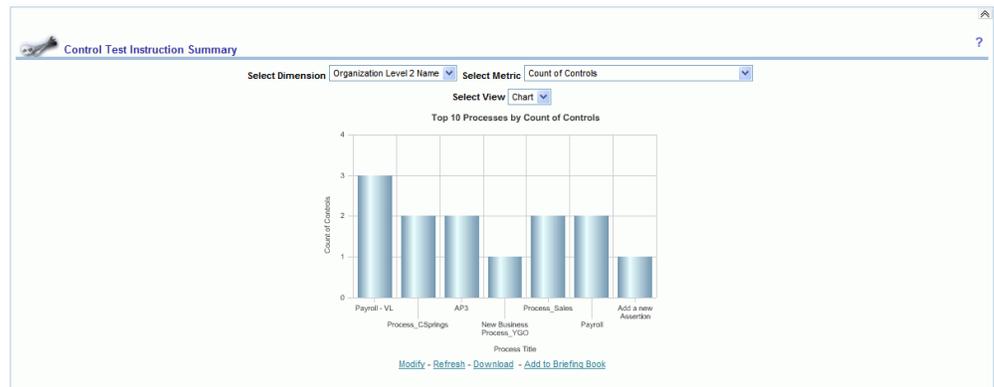
- **Controls without Test Instruction:**This is a landing report for Control Test Instruction Summary. In the Control Test Instruction Summary report when you click the values in Count of Controls without Test Instructions you will land on the Controls without Test Instruction report. This report enables the user to view all Controls with no Test Instructions.

Audit Planning Activities Tab

The Audit Planning Activities tab consists of the following reports by default, but you can customize the page to add custom reports if desired. There are two prompts: Process Type and Control Type. You can also choose to filter the reports by Test Plan Title, Process Title, Assertion Title, and Control Title.

- **Audit Test Control Detail:**This report allows the user to view details of Control Tests included in Audit Test Plans, along with Assertions.

- **Control and Test Instruction:**This report enables the user to view all Controls with details of related Test Instructions, as well as Canceled Results.

- **Test Instruction Detail:**This report displays details of Test Instructions such as Title, Description, Type, Approach and Success Criteria.

Oracle BI Publisher (BIP) Reports

Most of the GRCM based GRCI reports have been converted utilizing Oracle BI Publisher. Although the functional content and definition in each report type is the same, the look and feel of the BIP based reports is quite different from the OBIEE generated reports. The following is a complete list of all GRCM based BIP reports that are currently available:

Folder Name	Report Name	View Selector	Column Selector	# Templates

Assessment Reports	Regulatory Compliance Status	Report View Only	"Account Level 2 Name Organization Level 2 Name"	2
Assessment Reports	Design and Operating Effectiveness by Process	Report View Only	"Account Level 2 Name Organization Level 2 Name"	2
Audit and Process Test Reports	Non-Compliant Processes	Report View Only	"Account Level 2 Name Organization Level 2 Name"	2
Audit and Process Test Reports	Control Test Summary	Report View Only	"Account Level 2 Name Organization Level 2 Name"	2
Certification Reports	Certification Status	Report View Only	"Account Level 2 Name Organization Level 2 Name"	2
Certification Reports	Open Assessments by Due Date	Report View Only	"Account Level 2 Name Organization Level 2 Name"	2
Certification Reports	Assessment Status By Process Owner	Report View Only	"Account Level 2 Name Organization Level 2 Name"	2
Controls Reports	Controls Summary	Report View Only	"Account Level 2 Name Organization Level 2 Name"	2
Controls Reports	Controls Count - Summary	Report View Only	"Account Level 2 Name Organization Level 2 Name (show all the below metrics) Automated Control Count Preventative Control Count Manual Control Count Detective Control Count Key Control Count Subordinate Control Count Corrective Control Count"	2

Controls Reports	Accounts Lacking Mitigating Controls	Report View Only	"Account Level 2 Name Organization Level 2 Name"	2
Controls Reports	Processes With Control Issues	Report View Only	No	1
Controls Reports	Controls Test Failures	Report View Only	"Account Level 2 Name Organization Level 2 Name"	2
Issue Reports	Issues Scorecard Summary	Report View Only	"Account Level 2 Name Organization Level 2 Name"	2
Issue Reports	Audit and Process Test Issues	Report View Only	"Account Level 2 Name Organization Level 2 Name"	2
Issue Reports	Issues By Owner	Report View Only	"Account Level 2 Name Organization Level 2 Name"	2
Risk Maps	Risk Heat Map - Business Processes	Report View Only	No	1
Risk Maps	Risk Heat Map - Process Issues	Report View Only	No	1
Risk Maps	Risk Heat Map - Controls	Report View Only	No	1
Risk Maps	Risk Heat Map - Control Issues	Report View Only	No	1
Risk Reports	Risk by Process Owners	Report View Only	"Account Level 2 Name Organization Level 2 Name"	2
Risk Reports	Control Failure By Process	Report View Only	"Account Level 2 Name Organization Level 2 Name"	2

Risk Reports	Risks by Process - Issues Aging	Report View Only	"Account Level 2 Name Organization Level 2 Name"	2
Risk Reports	High Risk Processes With Issues	Report View Only	"Account Level 2 Name Organization Level 2 Name"	2
Risk Reports	High Risk Processes With No Controls Tested	Report View Only	No	1
Risk Reports	Number of Controls By Risk Type and Significance	Report View Only	"Account Level 2 Name Organization Level 2 Name (show all the below metrics) Automated Control Count Preventative Control Count Manual Control Count Detective Control Count Key Control Count Subordinate Control Count Corrective Control Count Monitoring Control Count"	2
Risk Reports	Number of Controls Failures By Risk Type	Report View Only	"Account Level 2 Name Organization Level 2 Name"	2

> **Note:** The installation and configuration of BIP reports is explained in detail in the GRCI Installation Guide and should be referred to for questions relating to these topics.

BIP Reports Characteristics

· All dimension views that are available in OBIEE have not been included in BIP reports. Only the Organization and Account views are implemented if available. These dimension views can be accessed by changing the template of the report as shown below.
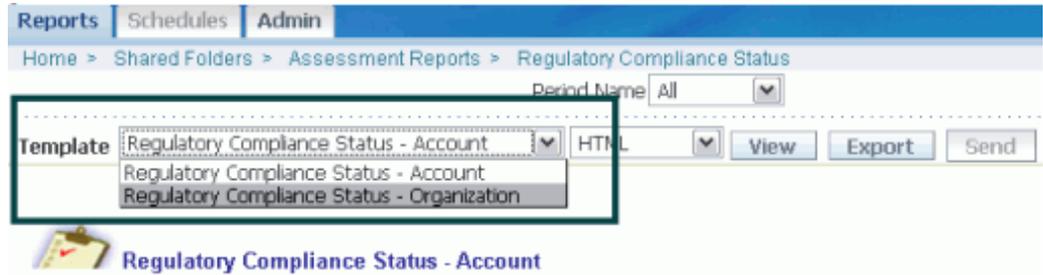
Unlike OBIEE reports, the BIP reports do not refresh automatically when prompt values are changed. You must click on the "View" button to see the changes to the report.
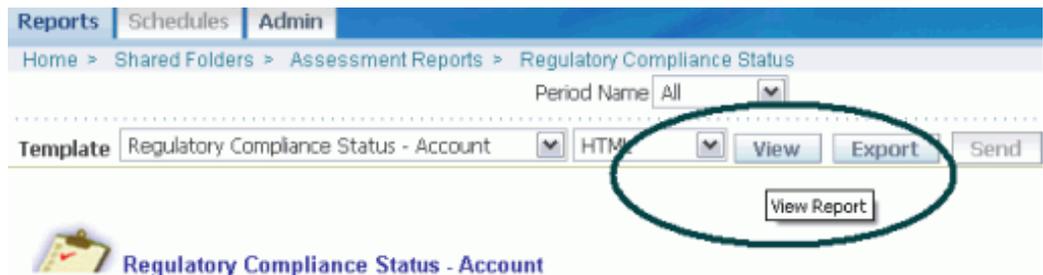
Most of the dashboard level prompts available in OBIEE have been implemented in BIP.
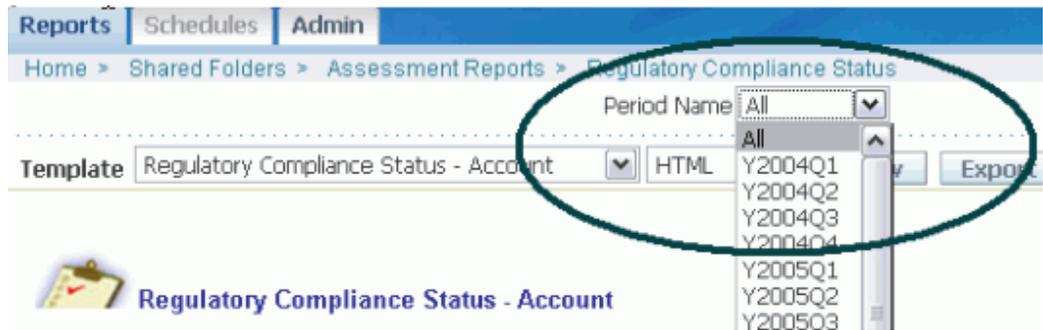
BIP reports can be customized if required. It requires change to the database query and the templates. Customization should include modification to the supplied xlf files if multi-language support is desired.

Limitations of BIP

- Drill to source application is not possible in BIP. (eg Process details or Control Details etc.)

- BIP does not provide any drill capabilities. Hence the BIP reports show the data at the most granular level. All the hierarchies present have been fully exploded.

- Conditional formatting of data is not possible in BIP.

- Representation of data in Pivot table format is not possible in BIP.

- Dashboards creation facility not available in BIP.

3

Application Access Control Dashboards

SOD Policy Dashboard

The SOD Policy Dashboard consists of two tabs:

- Overview

- Details
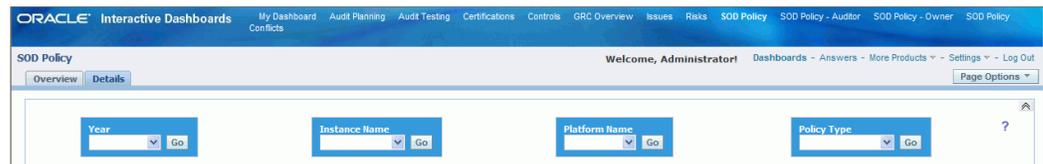
Overview Tab

The SOD (Segregation of Duties) Policy Dashboard Overview Tab consists of the following reports by default, but you can customize the page to add custom reports if desired. You can also choose to limit the reports by Year, Instance Name, Platform Name, and Policy Type using the dashboard prompts:

- **Policy Distribution by Application:**

  This report details by application area the distribution of SOD Policies for the current and prior year as well the percent change. This report drills to the SOD Policy Summary report.

- **SOD Policy Summary – Active in Current Year:** This report provides an overall summary view of an SOD Policy covering the policy name, owner, status, and priority. This report drills to the SOD Policy Exclusions report.

- **SOD Policy Exclusions:** This report details by SOD Policy the exclusions associated with the policy and the type of exclusions (Policy Level or Global).

- **SOD Policy Trend:**

  This report shows the trend of the number of SOD Policies by policy type and access point type.
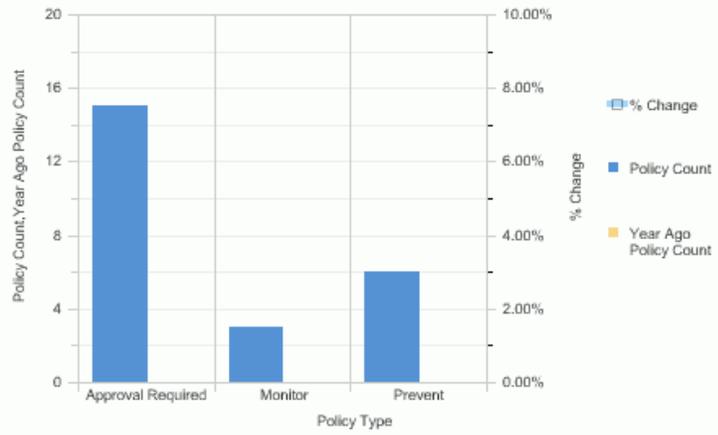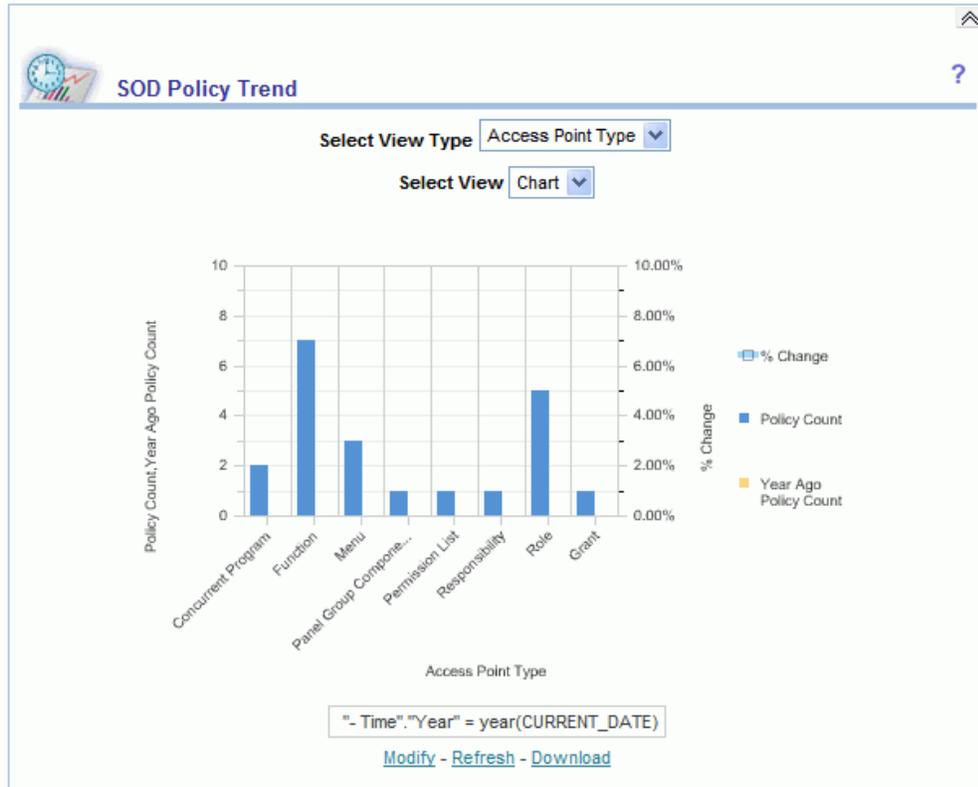
- **SOD Policy Count:**

  This report details the distribution of SOD Policies over key dimensions (for example, SOD Policy Type, Risk, Process).

- **SOD Policy Summary:** This report provides an overall summary view of an SOD Policy covering the policy name, owner, status, and priority. This report drills to the SOD Policies Exclusions report.

Details Tab

The SOD Policy Details Tab displays the following reports by default, but you can customize the page to add custom reports if desired. You can also choose to limit the

reports by Year, Instance Name, Platform Name, and Policy Type using the dashboard prompts:

- **Entitlement Exposure by SOD Policy Count :**

  This report shows the top ten SOD Policy entitlements that are associated with an SOD Policy.

- **Policy Detail:** This report is the drill report from Entitlement Exposure by SOD Policy Count and contains the Policy Details.

- **SOD Policy Effective Date Tracking:**

  This report tracks when an SOD Policy will become effective and provides a counter of days remaining until the SOD Policy becomes active.

SOD Policy Effective Date Tracking

Policy Type	Policy ID	Policy Name	Priority	Effective Date	Days Till Effective Date ▼
Monitor	241	Policy 001	1	8/13/2008 7:03:12 PM	(2)
Prevent	223	Test Policy S2	1	8/12/2008 8:05:13 PM	(3)
Monitor	225	Test Policy I2	2	8/12/2008 8:34:04 PM	(3)
Approval Required	222	Test Policy S1	2	8/12/2008 7:26:37 PM	(3)
Prevent	221	Test Policy 4 Inc	1	8/12/2008 7:25:24 PM	(3)
Approval Required	229	TEST1_PS	1	8/12/2008 9:02:49 PM	(3)
Prevent	227	Test Policy 12 Inc	2	8/12/2008 8:44:12 PM	(3)
Prevent	224	Test Policy 4-Trend	1	8/12/2008 8:33:40 PM	(3)
Prevent	231	TEST3_PS	1	8/12/2008 9:05:18 PM	(3)
Prevent	228	Test Policy I3	2	8/12/2008 8:47:00 PM	(3)

Records 1 - 10

TIMESTAMPDIFF(SQL_TSI_DAY , CURRENT_DATE , Policy Effective Date) is less than or equal to **-1**

Modify - Refresh - Download

- **High Priority SOD Policies By Business Processes:**

    This report shows High Priority SOD Policies, policy type, priority and associated business processes.

High Priority SOD Policies By Business Processes

Process	Policy Type	Policy Name	Policy Priority	Policy Owner User Name	Generic Dim Type
Capital and Risk	Monitor	Test PSFT Pol 04	2	admin	Business Process
Financial Close and Reporting	Approval Required	Test PSFT Pol 01	1	admin	Business Process
Human Resources	Prevent	Test EBS Pol 02	1	admin	Business Process
Logistics	Prevent	Test EBS Pol 03	2	admin	Business Process
Manufacturing	Prevent	Test EBS Pol 02	1	admin	Business Process
Order to Cash	Prevent	Test EBS Pol 02	1	admin	Business Process
Procure to Pay	Approval Required	Test EBS Pol 01	1	admin	Business Process
Support Services	Monitor	Test PSFT Pol 03	2	ssamudra	Business Process

Request contains **no filters**

Modify – Refresh – Download

- **Top 10 Policy Exclusions:**

  This report details the top 10 policy exclusion types (and their values) associated with SOD Policies and the count of policies for each exclusion type.

- **Top 10 Policy Exclusions – Policy Summary:** This report is displayed when the user drills on report values to view detail information from the Top 10 Policy Exclusions report.

SOD Policy - Auditor Dashboard

The SOD Policy - Auditor Dashboard consists of two tabs:

- Overview

- Details

Overview Tab

The SOD Policy - Auditor Overview Tab displays the following reports by default, but you can customize the page to add custom reports if desired. You can also choose to limit the reports by Year, Instance Name, Platform Name, Policy Type and Access Point Type using the dashboard prompt:

- **SOD Policy Conflicts by User:**

  This report provides a multi-drill path capability to analyze SOD Policy conflicts by User, Access Point and SOD Policy. Users can select specific Application User(s) using the report prompt.

- **SOD Policy Conflicts by User – Policy Access Point & Role:** This report provides capability to analyze SOD Policy Conflicts by Application User and Policy Type. The data can be viewed by Policy Name, Access Point Name - Privilege, or Access Point Name - Role by selecting the desired dimension from the LOV.

- **SOD Violation by Policy Type and Role:**

    This report shows SOD Policy conflicts by Access Point Name - Role and Policy Type.

- **Distribution of Business Processes Across SOD Policies:**

  This report shows the distribution of Policy Counts by Process and Policy Type for an organization.

- **Distribution of Access points Across SOD Policies:**

  This report details the distribution of Access points distribution across SOD Policies.

Distribution of Business Processes Across SOD Policies

Process	Policy Type	Policy Count	Total Policy Count	Percentage of policies
Capital and Risk	Monitor	1	6	16.67%
Information System Management	Approval Required	2	6	33.33%
Logistics	Prevent	1	6	16.67%
Unassigned	Approval Required	2	6	33.33%

Modify - Refresh - Download

Distribution of Access points Across SOD Policies
(Drill on Policy Count to view SOD Policy information)

Select Dimension: Access Point Type

Select View: Chart

Policy Status is equal to **Active**
and Policy Count is in top **10**

Modify - Refresh - Download
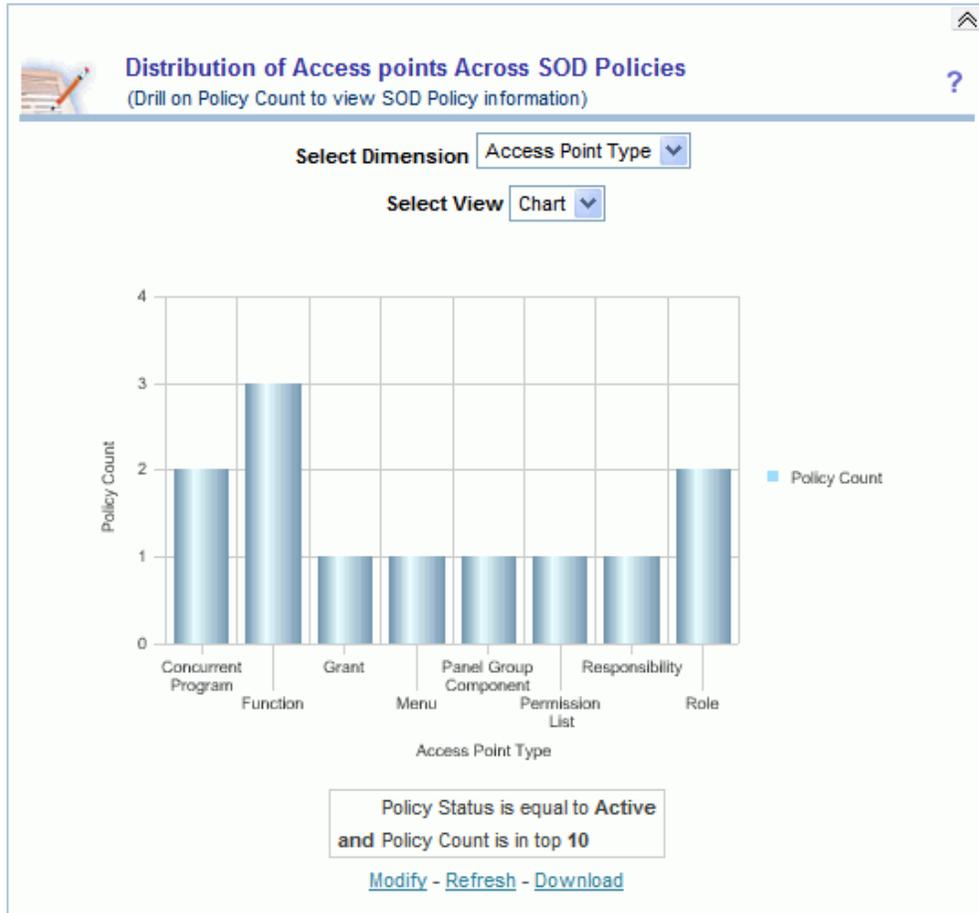
- **SOD Policy Summary:** This report provides an overall summary view of an SOD Policy including the policy name, owner, status, and priority. This report drills to the SOD Policy Exclusions report.

- **SOD Policy Exclusions:** This report details by SOD Policy the exclusions associated with the policy and the type of exclusions (Policy Level or Global).

Details Tab

The SOD Policy - Auditor Details Tab displays the following reports by default, but you can customize the page to add custom reports if desired. You can also choose to limit the reports by Year, Instance Name, Platform Name, Policy Type and Access Point Type using the dashboard prompts:

- **Conflict Count for Application User:**

  This report shows the conflict Path Count and App User Conflict Count by Policy Type and Application User.

- **SOD Conflict Path Detail – Application User:** This report shows the SOD Policy Conflict Path detail information relating to the conflict (e.g., application user, conflict path, run date, status, etc.).

- **Top 10 Offending Access Points - Privileges:**

This report shows the Top 10 offending Access Points by Privileges. Users can select

a specific application user name(s) using the report prompt.

- **SOD Conflict Path Detail – Privilege:** This report shows the SOD Policy conflict detail information relating to the conflict (e.g., user, conflict path, run date, status, etc.).

- **Top 10 Offending Access Points - Roles:**

  This report summarizes the number of SOD Conflicts, SOD Conflict Paths, and SOD Policies that relate the Access Point to the Role. Users can select a specific access point name - privileges using the report prompt.

- **SOD Conflict Path Detail – Role:** This report shows the SOD Policy conflict detail information relating to the conflict (e.g., user, conflict path, run date, status, etc.).

- **SOD Policy Violations By Conflict Run:**

  This report shows all approved SOD Policy conflict paths by Access Point and SOD Policy Type and by the person assigned to resolve the SOD Policy conflict.

- **SOD Conflict Path Detail:** This report shows the conflict path detail information by person assigned to resolve (e.g., user, conflict path, run-date, privilege, etc.).

- **Pending Conflicts That Are Outstanding:** This report shows all pending SOD Policy conflict paths by the person assigned to resolve the SOD Policy conflict and how long the SOD Conflict has had the status of pending.

SOD Policy - Owner Dashboard

The SOD Policy - Owner Dashboard consists of two tabs:

- Overview

- Details
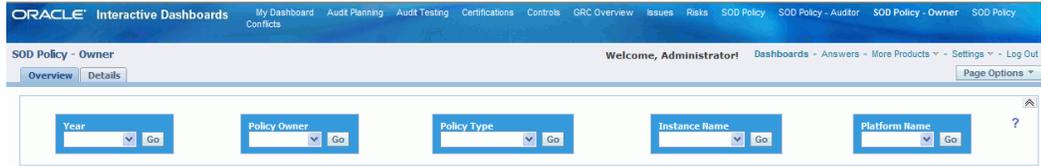
Overview Tab

The SOD Policy - Owner Dashboard Overview Tab displays the following reports by default, but you can customize the page to add custom reports if desired. You can also choose to limit the reports by Year, Policy Owner, Policy Type, Instance Name, and Platform Name using the dashboard prompts.

- **Distribution of SOD Policy Conflicts:**

  This report shows Distribution of Assigned SOD Policy Conflicts by the person to whom they are assigned.

- **Distribution of SOD Policy Conflicts by Policy Type:** This report shows SOD policy conflicts by app user conflict count and policy type.

SOD Policy - Owner

Distribution of SOD Policy Conflicts by Policy type
(Drill on App User Conflict Count to view SOD Conflict Path Detail report)

Select View | Chart
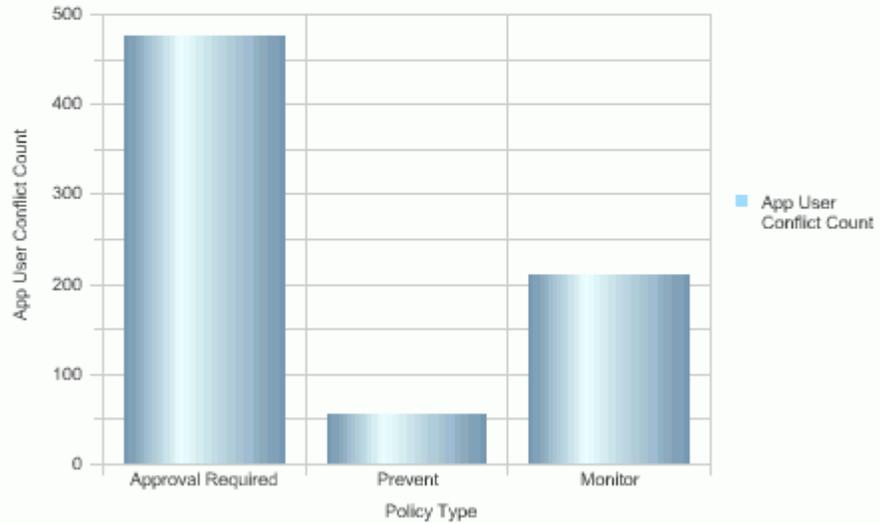
User Name is equal to **admin**

- **SOD Conflict Path Detail:** This report shows the conflict path detail information by person assigned to resolve(e.g., user, conflict path, rundate, privilege, etc.).

SOD Policy - Owner   Welcome, Administrator! Dashboards - Answers - Mor

SOD Conflict Path Detail
(Drill on Conflict Path Status to View DaysOutstanding)

Related User Name	Assigned to User	Policy ID	Policy Name	Policy Type	Conflict Path ID	Total Conflict Path Count	Run Date	Run Id	Privileges	Conflict Path Status
ABOASE	admin	22	Test EBS Pol 05	Approval Required	2102		1	4/16/2009	22	System Controls	Pending
ABOASE	admin	3	Test EBS Pol 01	Approval Required	1		1	3/24/2009	1	Procurement Card Transactions	Pending
ABOASE	admin	3	Test EBS Pol 01	Approval Required	1194		1	3/24/2009	5	Procurement Card Transactions	Pending
ABOASE	admin	3	Test EBS Pol 01	Approval Required	1195		1	3/24/2009	5	ABC Groups	Pending
ABOASE	admin	3	Test EBS Pol 01	Approval Required	1196		1	3/24/2009	5	Procurement Card Transactions	Pending
ABOASE	admin	3	Test EBS Pol 01	Approval Required	1197		1	3/24/2009	5	ABC Groups	Pending
ABOASE	admin	3	Test EBS Pol 01	Approval Required	1567		1	3/25/2009	8	Procurement Card Transactions	Pending
ABOASE	admin	3	Test EBS Pol 01	Approval Required	1568		1	3/25/2009	8	ABC Groups	Pending
ABOASE	admin	3	Test EBS Pol 01	Approval Required	1569		1	3/25/2009	8	Procurement Card Transactions	Pending
ABOASE	admin	3	Test EBS Pol 01	Approval Required	1570		1	3/25/2009	8	ABC Groups	Pending

Records 1 - 10

User Name is equal to **admin**
and Policy Type is equal to **Approval Required**

- **Pending Conflicts That Are Outstanding:** This report shows all pending SOD Policy conflict paths by the person assigned to resolve the SOD Policy conflict and how long the SOD Conflict has had the status of pending.

SOD Policy - Owner   Welcome, Adr

Pending Conflicts That Are Outstanding

Policy Owner User Name	Assigned To	Conflict Path Status	Conflict Path ID	Days Outstanding	Run Date
admin	admin	Pending	1196	22	3/24/2009

Conflict Path Status is equal to **Pending**
and User Name is equal to **admin**
and Conflict Path ID Link is equal to 1196
and Run Id is equal to **5**
and Related User Name is equal to **ABOASE**
and Policy Type is equal to **Approval Required**
and Policy Name is equal to **Test EBS Pol 01**

Return – Modify – Refresh – Download – Create Bookmark Link

- **SOD Policy Conflicts - Top 10 Application Users:**

  This report shows the Top 10 Application Users who have violated SOD Policies on a current and year ago basis by Access Point Type and SOD Policy Type.

SOD Policy Conflicts - Top 10 Application Users
(Drill on App User Conflict Count to view details by Policy Type/Access Point Type)

Year	Global User Name	Application User Name	App User Conflict Count	Year Ago App User Conflict Count
2009	EBUSINESS	EBUSINESS	2	0
2009	WIZARD	WIZARD	2	0
2009	TREASURER	TREASURER	2	0
2009	ABOASE	ABOASE	1	0
2009	ADB	ADB	1	0
2009	AGENT01	AGENT01	1	0
2009	AGENT02	AGENT02	1	0
2009	ALAN	ALAN	1	0
2009	AMONTEIRO	AMONTEIRO	1	0
2009	ANTON	ANTON	1	0

Records 1 - 10

App User Conflict Count is in top **10**

Modify - Refresh - Download

- **SOD Policy Conflicts – Top 10 Application Users – Detail:** This report shows the Top 10 Application Users who have violated SOD Policies on a current and year ago basis by Access Point Type and SOD Policy Type.

- **SOD Policy Violations By Conflict Run:**

  This report shows all approved SOD Policy conflict paths by Access Point and SOD Policy Type and by the person assigned to resolve the SOD Policy conflict.

- **SOD Conflict Path Detail:** This report shows the conflict path detail information by person assigned to resolve(e.g., user, conflict path, rundate, privilege, etc.).

- **Pending Conflicts That Are Outstanding:** This report shows all pending SOD Policy conflict paths by by the person assigned to resolve the SOD Policy conflict and how long the SOD Conflict has had the status of pending.

- **Top 10 Policy Exclusions:**

  This report details the top 10 policy exclusion types (and their values) associated with SOD Policies and the count of policies for each exclusion type.

- **Top 10 Policy Exclusion – Policy Summary:** This report gives the summary for the policies that are connected to the exclusion drilled from.

Details Tab

The SOD Policy - Owner Dashboard Details Tab displays the following reports by default, but you can customize the page to add custom reports if desired. You can also choose to limit the reports by Year, Policy Owner, Instance Name, Platform Name and

Policy Type using the dashboard prompts:

- **SOD Policy Modification Tracking:**

  This report tracks all SOD policies by SOD Policy Owner that have been modified during a given year.
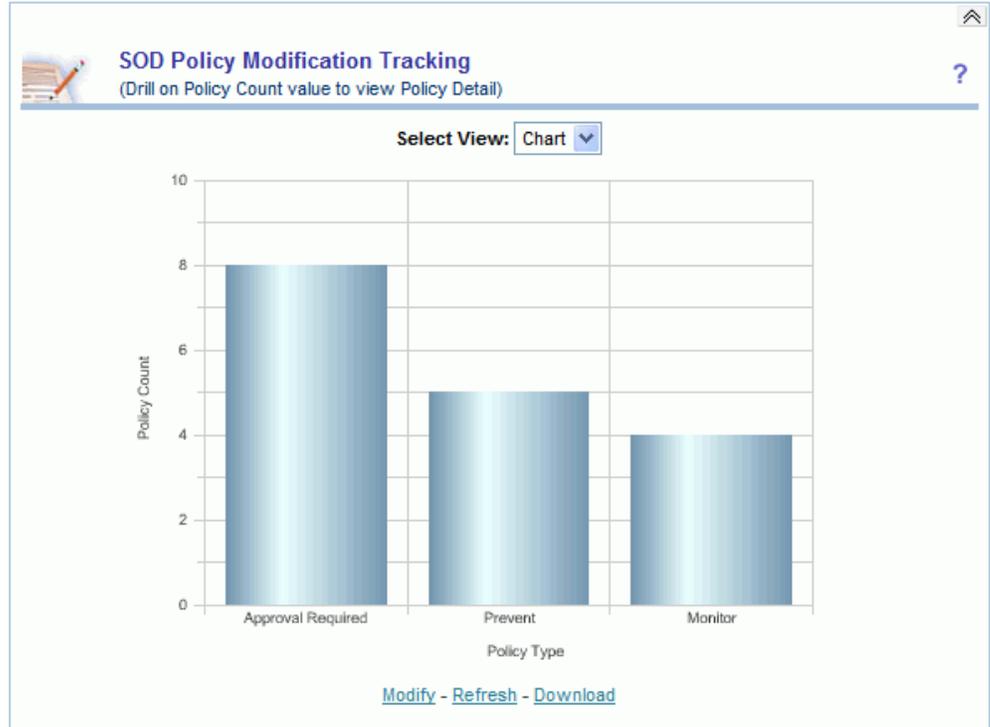
- **Policy Detail:** This report is the drill down from SOD Policy Modification Tracking and contains policy details and information.

- **Conflicts by SOD Policy:**

  This report shows the total conflict count by run id and date, and policy details and information.

- **Conflicts by SOD Policy and Application:** This drill down report shows the application user conflict count and conflict path count by run, and policy and platform/instance.

- **SOD Conflict Path Detail – Application User:** This drill down report shows the SOD Policy Conflict Path detail information relating to the conflict including: policy type, id, and name; run date and id; conflict path id; global user name and related user's name; and conflict status.

- **SOD Policy Conflicts with Approved Status:**

  This report shows all approved SOD Policy conflicts paths by Access Point Type and also provides a count of conflict path.

- **SOD Conflict Burndown:**

  This report shows by conflict analysis run the current and previous number of conflicts, the difference and the % change.

- **SOD Policy Effective End Date Tracking:**

  This report tracks when an SOD Policy is to become effective and provides a counter of days remaining until the SOD Policy becomes active.

SOD Policy Conflicts Dashboard

The SOD Policy Conflicts Overview Dashboard consists of two tabs:

- Overview

- Details

Overview Tab

The SOD Policy Conflicts Dashboard Overview Tab displays the following reports by default, but you can customize the page to add custom reports if desired. You can also choose to limit the reports by Year, Platform Name, Instance Name, and Access Point Type:

- **Application Access Status:**

    This report shows by application (e.g., Oracle or Peoplesoft) the current and previous application user conflict counts and the percentage change.

    It shows the Top 10 rows for policy-run for a platform and/or instance with highest percent change.
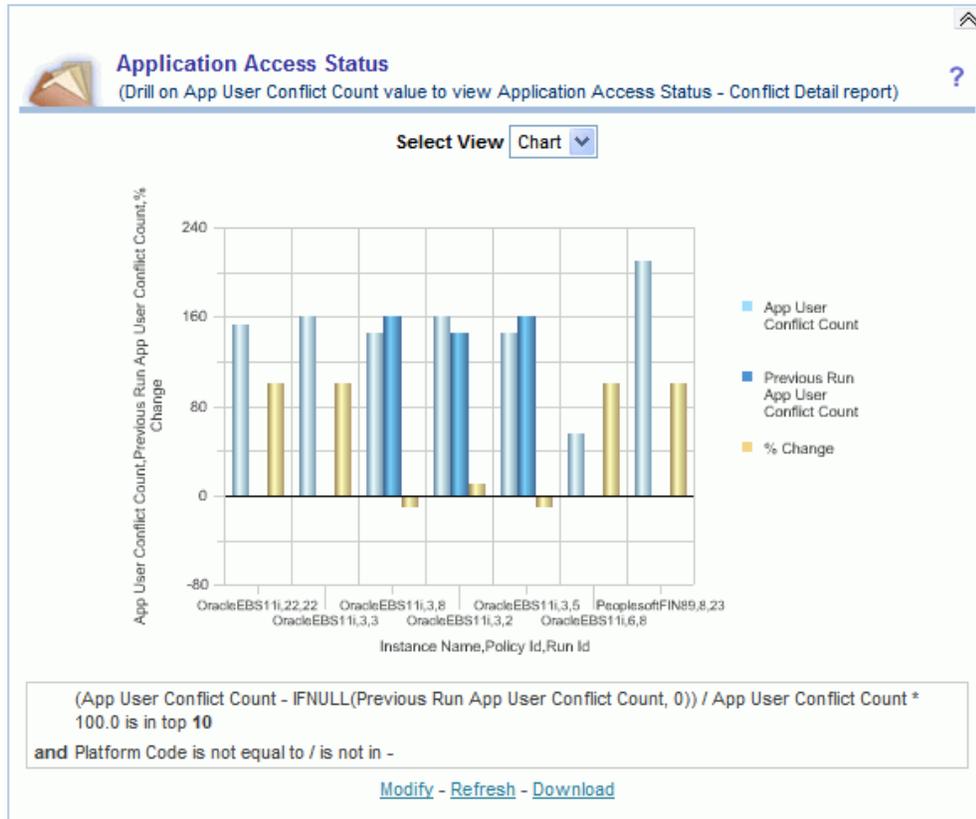
- **Application Access Status – Conflict Detail:** This report shows the conflicts for an application user within a platform for a policy for a specific run.

Application Access Status - Conflict Detail   ?

Platform Name	Instance Name	Policy ID	Policy Name	Run Id	Global User Name	Related User Name	App User Conflict Count
						Al Approver (AL)	1
						Anna Anderson (EB1)	1
						Anne Approver (ANNE)	1
						Anthony,Marienella (BIA3)	1
						Art Approver (ART)	1
						Bank Manager (TRBM1)	1
						Becker,Angela (EGM1)	1
						Becker,Christine (APA2)	1
						Beeler,Thomas (GLA3)	1
						Betsy Maertens (SSC2)	1
						Blake,Scott (POS1)	1
						Bob U. Young (BOBYOUNG)	1
PeopleSoft	PeoplesoftFIN89	8	Test PSFT Pol 04	23	Al Approver (AL)	Boyer,Sarah (INA3)	1
						Brown,James (EGD1)	1
						Bukau,Hans (APS4)	1
						Buyer Accountant (BUYACCT)	1
						Buyer Approver 1 (BUYAPPR1)	1
						Buyer Approver 2 (BUYAPPR2)	1
						Buyer Approver 3 (BUYAPPR3)	1
						Buyer Match Manager (BUYMTCH)	1
						Buyer Treasurer (BUYTREAS)	1
						Callis,Betty (INS1)	1
						Camilla Contact (CAMILLA)	1
						Caroline Contact (CAROLINE)	1
						Cash Manager (TRCM1)	1

◄◄ ◄   ► ►*   Records 1 - 25

Platform Name is equal to **PeopleSoft**
and Instance Name is equal to **PeoplesoftFIN89**
and Run Id is equal to **23**
and Policy Id is equal to **8**
and Platform Code is not equal to / is not in –

- **Conflicts by Access Point:**

  This report shows by Access Point (Role & Privilege) and Policy Type the total conflict paths and their percentage breakdown.

- **Distribution of SOD Policy Conflicts:**

  This report shows by the person assigned to resolve an SOD Policy conflict the distribution of assigned SOD Policy conflicts.

- **SOD Conflict Path Detail:** This report shows the conflict path detail information by person assigned to resolve(e.g., user, conflict path, rundate, privilege, etc.).

SOD Policy Conflicts Welcome, Administrator!

SOD Conflict Path Detail - Application User ?

Policy Type	Policy ID	Policy Name	Run Date	Run Id	Conflict Path ID	Global User Name	Related User Name	Total Conflict Path Count	Conflict Path Status
Approval Required	3	Test EBS Pol 01	3/24/2009	1	273	ANTON	ANTON	1	Pending
Approval Required	3	Test EBS Pol 01	3/24/2009	1	273	ANTON	DIANA KROYTOR	1	Pending
Approval Required	3	Test EBS Pol 01	3/24/2009	1	273	ANTON	DIANA_KROYTOR	1	Pending
Approval Required	3	Test EBS Pol 01	3/24/2009	1	273	ANTON	DK_ABM	1	Pending
Approval Required	3	Test EBS Pol 01	3/24/2009	1	273	ANTON	DK_NEW_ORA	1	Pending
Approval Required	3	Test EBS Pol 01	3/24/2009	1	273	ANTON	ER14	1	Pending
Approval Required	3	Test EBS Pol 01	3/24/2009	1	42	ANTON	ANTON	1	Pending
Approval Required	3	Test EBS Pol 01	3/24/2009	1	42	ANTON	DIANA KROYTOR	1	Pending
Approval Required	3	Test EBS Pol 01	3/24/2009	1	42	ANTON	DIANA_KROYTOR	1	Pending
Approval Required	3	Test EBS Pol 01	3/24/2009	1	42	ANTON	DK_ABM	1	Pending

Records 1 - 10

Policy Type is equal to **Approval Required**
and Policy Name is equal to **Test EBS Pol 01**
and Run Id is equal to **1**
and Global User Name is equal to **ANTON**
and Policy Id is equal to **3**
and Time Date is equal to date **'2009-03-24'**

- **Pending Conflicts That Are Outstanding:** This report shows all pending SOD Policy conflict paths by the person assigned to resolve the SOD Policy conflict and how long the SOD Conflict has had the status of pending.

SOD Policy Conflicts Welcome, Adr

Pending Conflicts That Are Outstanding ?

Policy Owner User Name	Assigned To	Conflict Path Status	Conflict Path ID	Days Outstanding	Run Date
ssamudra	admin	Pending	2105	0	4/16/2009

Instance Name is equal to **OracleEBS11i**
and Platform Name is equal to **Oracle**
and Conflict Path Status is equal to **Pending**
and User Name is equal to **admin**
and Conflict Path ID Link is equal to 2105
and Run Id is equal to **22**
and Related User Name is equal to **AOLCLASS**
and Policy Type is equal to **Approval Required**
and Policy Name is equal to **Test EBS Pol 05**

- **SOD Conflict Burndown:**

This report shows by conflict analysis run the current and previous number of conflicts, the difference and the % change.
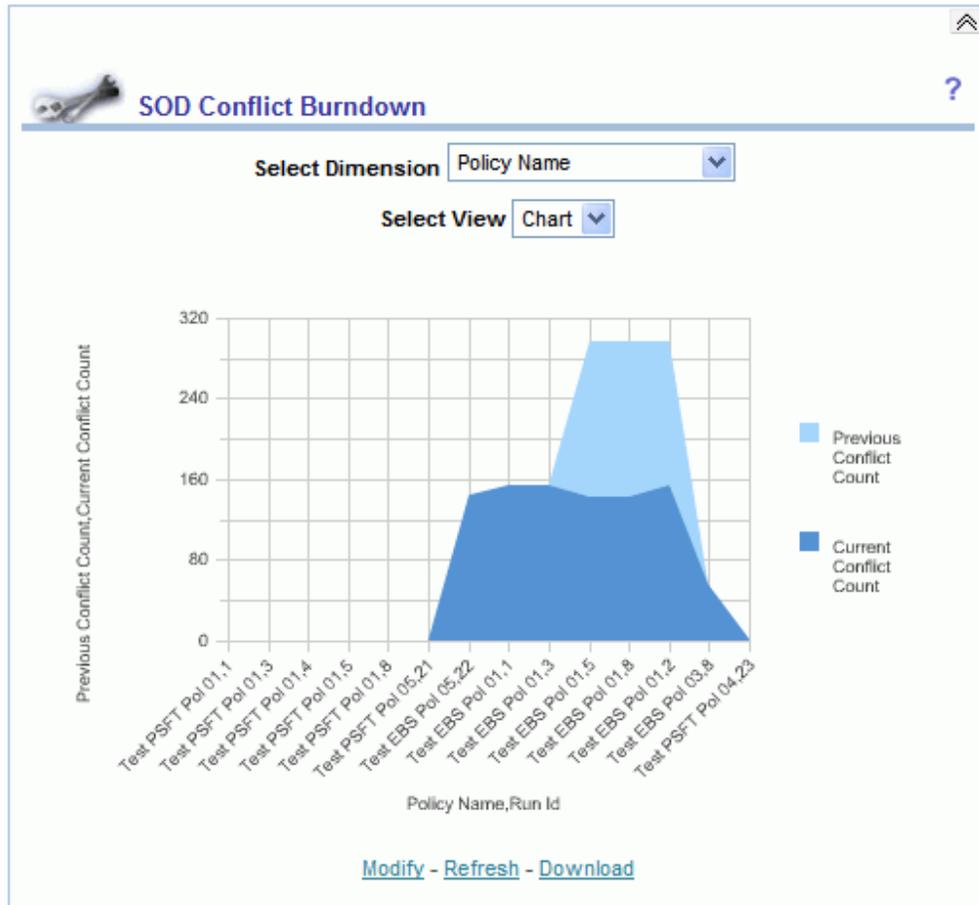
- **Conflicts by Status:**This report shows the global user conflict count, and the related status by run, policy, and global user.

Conflicts by Status
(Drill on Total Conflict Count to view 'SOD Conflict Path Detail – Application User' report)

Run Id	Run Date	Policy Type	Policy Name	Policy Id	Conflict Status	Global User Name	Total Conflict Count
1	3/24/2009	Approval Required	Test EBS Pol 01	3	Pending	ABOASE	1
1	3/24/2009	Approval Required	Test EBS Pol 01	3	Pending	ADB	1
1	3/24/2009	Approval Required	Test EBS Pol 01	3	Pending	ALAN	1
1	3/24/2009	Approval Required	Test EBS Pol 01	3	Pending	AMONTEIRO	1
1	3/24/2009	Approval Required	Test EBS Pol 01	3	Pending	ANTON	1
1	3/24/2009	Approval Required	Test EBS Pol 01	3	Pending	ARABIC	1
1	3/24/2009	Approval Required	Test EBS Pol 01	3	Pending	ARGENTINA	1
1	3/24/2009	Approval Required	Test EBS Pol 01	3	Pending	BAISHENGCHANG	1
1	3/24/2009	Approval Required	Test EBS Pol 01	3	Pending	BALLEN	1
1	3/24/2009	Approval Required	Test EBS Pol 01	3	Pending	BANKING	1

Records 1 - 10

Modify - Refresh - Download

- **SOD Conflict Path Detail – Application User:** This report shows the SOD Policy Conflict Path detail information relating to the conflict (e.g., application user, conflict path, run date, status, etc.).

SOD Policy Conflicts   Welcome, Administrator!

SOD Conflict Path Detail - Application User

Policy Type	Policy ID	Policy Name	Run Date	Run Id	Conflict Path ID	Global User Name	Related User Name	Total Conflict Path Count	Conflict Path Status
Approval Required	3	Test EBS Pol 01	3/24/2009	1	22	AMONTEIRO	AMONTEIRO	1	Pending
Approval Required	3	Test EBS Pol 01	3/24/2009	1	24	AMONTEIRO	AMONTEIRO	1	Pending
Approval Required	3	Test EBS Pol 01	3/24/2009	1	29	AMONTEIRO	AMONTEIRO	1	Pending
Approval Required	3	Test EBS Pol 01	3/24/2009	1	31	AMONTEIRO	AMONTEIRO	1	Pending
Approval Required	3	Test EBS Pol 01	3/24/2009	1	33	AMONTEIRO	AMONTEIRO	1	Pending
Approval Required	3	Test EBS Pol 01	3/24/2009	1	35	AMONTEIRO	AMONTEIRO	1	Pending
Grand Total								**6**	

Policy Type is equal to **Approval Required**
and Policy Name is equal to **Test EBS Pol 01**
and Run Id is equal to **1**
and Global User Name is equal to **AMONTEIRO**
and Policy Id is equal to **3**
and Time Date is equal to date **'2009-03-24'**

Detail Tab

The SOD Policy Conflicts Dashboard Detail Tab displays the following reports by default, but you can customize the page to add custom reports if desired. You can also choose to limit the reports by Year, Platform Name, Instance Name, and Access Point Type:

- **SOD Policy Conflicts with Approved Status:**

  This report shows all approved SOD Policy conflicts paths by Access Point Type and also provides a count of conflict path.

SOD Policy Conflicts with Approved Status

Policy Owner User Name	Application User Name	Access Point Type	Total Conflict Path Count	Year Ago Total Conflict Path Count
admin	HCSYSADM	Function	1	
admin	HRMS	Function	4	
admin	OMSUPV	Function	4	
admin	SYSADMIN	Function	6	

Conflict Path Status is equal to **Approved**

Modify - Refresh - Download

- **Pending Conflicts That Are Outstanding:**

  This report shows all pending SOD Policy conflict paths by the person assigned to resolve the SOD Policy conflict and how long the SOD Conflict has had the status of pending.

Pending Conflicts That Are Outstanding

Policy Owner User Name	Assigned To	Conflict Path Status	Conflict Path ID	Days Outstanding	Run Date
admin	admin	Pending	134773	2	8/12/2008
admin	admin	Pending	118427	2	8/12/2008
admin	admin	Pending	127179	2	8/12/2008
admin	admin	Pending	180142	2	8/12/2008
admin	admin	Pending	180750	2	8/12/2008
admin	admin	Pending	130226	2	8/12/2008
admin	admin	Pending	183553	2	8/12/2008
admin	admin	Pending	120512	2	8/12/2008
admin	admin	Pending	159402	2	8/12/2008
admin	admin	Pending	204587	2	8/12/2008

Records 1 - 10

Conflict Path Status is equal to **Pending**

Modify - Refresh - Download

- **SOD Policy Conflicts by User:**

This report provides a multi-drill path capability to analyze by user SOD Policy conflicts by the name of the application user, type of policy approval required, and the count of policy violations.

- **SOD Policy Conflicts by User – Policy, Access Point & Role:** This drill down report provides capability to analyze SOD Policy Conflicts by Application User and Policy Type. The data can be viewed by Policy Name, Access Point Name - Privilege, or Access Point Name - Role by selecting a dimension from the LOV.

- **Top 10 Access Points by SOD Policy Conflict Paths:**

This report shows the Top 10 Access Points, the count of SOD Policy conflict paths, and the percentage breakdown.

Top 10 Access Points by SOD Policy Conflict Paths

?

Select Access Point | Access Point Name - Privileges ▾

Privilege Name	Conflict Path Count ▾	Total Conflict Path Count %
ABC Groups	2974	52.24%
Procurement Card Transactions	1701	29.88%
Project Owner	211	3.71%
Invoices	205	3.60%
System Controls	204	3.58%
Schedule Orders	110	1.93%
Cancel Orders	108	1.90%
Void Payments Report	90	1.58%
Purge	44	0.77%
Define Alert	32	0.56%

Total Conflict Path Count is in top **10**

Modify – Refresh – Download

4

Repository Modeling for SOD Subject Areas

This chapter covers the following topics:

- Introduction
- Subject Area – SOD Detail
- Subject Area – SOD Conflicts
- Subject Area – SOD Policy
- Subject Area – SOD Policy Conditions
- Metrics
- Common SOD Dimensions
- SOD Conditions
- SOD Path Conditions

Introduction

To create error free reports and interactive dashboards, you need to understand the ways to consume the facts and dimensions in the respective subject areas. This chapter describes most of the possible combinations for using SOD facts and dimensions effectively to generate reports.

In GRI 2.0.1, subject areas are categorized as Overview and Detail. The overview subject areas are:

- SOD Conflicts
- SOD Policy
- SOD Policy Conditions

The detailed subject area is SOD Detail.

Subject Area – SOD Detail

The SOD Detail subject area includes the following folders:

- Common Dimensions

- SOD user conflict specific analytics

- SOD conflict path specific analytics

- SOD conflict analytics by run

- SOD policy

- Conditions

- Path conditions

Common Dimensions

Refer the Common Dimensions section of this chapter for details of common dimensions.

SOD User Conflict Specific Analytics

This folder contains the Fact - Global User Conflict. This fact joins with all dimensions in the Common Dimensions folder namely the Policy, Run and Time; the Global User Conflict fact should not be used in combination with any other dimensions as errors will result. The measures in this fact are related to Global users and not related users from the Application user dimension. All the measures related to Fact – Global User Conflict are listed in the table Global User Conflict Metrics in the Metrics section.

SOD Conflict Path Specific Analytics

This folder contains the following facts and dimensions:

- **Instance Dimension:** The Instance dimension in SOD Conflict Path Specific Analytics folder can also be used with dimensions and facts from the following folders.

  - SOD Conflict Analytics by Run

  - SOD Conflicts

  - SOD Policy

- Conditions

- Path Conditions

Do not use the Instance dimension with Fact - Global User Conflict as the metrics defined in this fact are not instance specific.

- **Application User Dimension**The Application user dimension in SOD Conflict Path Specific Analytics folder can also be used with dimensions and facts from the following folders.

  - SOD Conflicts

  - SOD Policy

  - Conditions

  - Path Conditions

  The Application User Dimension should not be used with the facts and dimensions in the SOD Conflict Analytics by Run folder. The Application User Dimension should be used with the Fact – Global User Conflict only; use it with reference to the attribute – Global user name.

- **Access Point – Role Dimension:** The Access Point – Role dimension (Role playing version of access point dimension) present in SOD Conflict Path Specific Analytics folder can also be used with dimensions and facts from the current folder and common dimensions only.

- **Access Point – Privileges Dimension:** The Access Point – Privileges dimension (Role playing version of access point dimension) present in SOD Conflict Path Specific Analytics folder can also be used with dimensions and facts from the current folder and common dimensions only.

- **Entitlement Dimension:** Entitlement is a group of access points in various combinations to define a policy. The entitlement dimension in SOD Conflict Path Specific Analytics folder can also be used with dimensions and facts from SOD Policy and common dimension. Note: Make sure that the entitlement dimension should not be used with dimensions and facts from folders:

  - Conditions

  - Path Conditions

  - SOD Conflict Analytics by Run

- **ACG User - Assigned To Dimension:** ACG users are auditors and policy owners. This dimension is used only in SOD Conflict Path Specific Analytics (current

folder).

- **Fact - Conflict:** The conflict fact joins with all the dimensions from Common Dimensions folder namely the Policy, Run and Time. All the measures calculated or derived in the conflict fact are specific to application user specific (Related user) and instance or platform. This fact should only be used in combination with any other dimensions in the current folder and common dimensions.

SOD Conflict Analytics by Run

This folder contains the following facts and dimensions which can be used in combination with Common dimensions only.

- **Previous Run:**The previous run dimension joins with the Fact – Policy Previous Run to provide the previous run details.

- **Time Day - Previous Run Date:**This dimension joins with the Fact – Policy Previous Run to provide the date of the previous run with respect to the current run.

- **Fact - Policy Previous Run:** The measures defined in this fact are with respect to current run (from common dimensions) and previous run (from previous run dimension) combination and also the time dimensions of Time Day - Previous Run Date and Time (from common dimensions).

SOD Policy

This folder contains Fact - SOD Policy. This fact joins with all the dimensions in from Common Dimensions folder namely the Policy, Run and Time. They should not be used in combination with any other dimensions as they result in error data.

Conditions

Refer to the Conditions section of this chapter.

Subject Area – SOD Conflicts

The SOD conflicts subject area has the following structure.

- Common Dimensions (for details, refer to the Common Dimensions section of this chapter.)

- SOD user conflict specific analytics

- SOD conflict path specific analytics

- SOD conflict analytics by run

SOD User Conflict Specific Analytics

This folder contains the Fact - Global User Conflict. This fact joins with all the dimensions in from Common Dimensions folder, namely the Policy, Run and Time. These dimensions should not be used in combination with any other dimensions as they result in error data. The measures in this fact are related to Global users and are not related to users from the Application user dimension. All measures related to Fact – Global User Conflict are listed in the table Global User Conflict Metrics in the Metrics section.

SOD Conflict Path Specific Analytics

This folder contains the following facts and dimensions:

- **Instance Dimension:**The Instance dimension in SOD Conflict Path Specific Analytics folder can also be used with dimensions and facts from the following folders:

    - SOD Conflict Analytics by Run

    - SOD Conflicts

    - SOD Policy

    - Conditions

    - Path Conditions

    Do not use Instance dimension with Fact - Global User Conflict as the metrics defined in this fact are not instance specific.

- **Application User Dimension:**The Application user dimension in SOD Conflict Path Specific Analytics folder should be used only with dimensions and facts in the current folder. The Application User Dimension should not be used with facts and dimensions in folder SOD Conflict Analytics by Run. The Application User Dimension should be used with Fact – Global User Conflict only with reference to the attribute – Global user name.

- **Access Point – Role Dimension:**The Access Point – Role dimension (Role playing version of access point dimension) present in SOD Conflict Path Specific Analytics folder can also be used with dimensions and facts from the current folder and common dimensions only.

- **Access Point – Privileges Dimension:**The Access Point – Privileges dimension (Role playing version of access point dimension) present in SOD Conflict Path

Specific Analytics folder can also be used with dimensions and facts from the current folder and common dimensions only.

- **Entitlement Dimension:** Entitlement is a group of access points in various combinations to define a policy. The entitlement dimension in SOD Conflict Path Specific Analytics should be used specific to this folder. Do not use the entitlement dimension with dimensions and facts from the SOD Conflict Analytics by Run folder.

- **ACG User - Assigned To Dimension:** ACG users are auditors and policy owners. This dimension is used only in SOD Conflict Path Specific Analytics (current folder).

- **Fact - Conflict:** The conflict fact joins with all the dimensions from Common Dimensions folder namely the Policy, Run and Time. All of the measures calculated or derived in the conflict fact are specific to application user specific (Related user) and instance or platform. Only use this fact in combination with any other dimensions in the current folder and common dimensions.

SOD Conflict Analytics By Run

This folder contains the following facts and dimension. These facts and dimensions must be used in combination with Common dimensions only:

- **Previous Run:** The previous run dimension joins with the Fact – Policy Previous Run to provide the previous run details.

- **Time Day - Previous Run Date:** This dimension joins with the Fact – Policy Previous Run to provide the date of the previous run with respect to the current run.

- **Fact - Policy Previous Run:** The measures defined in this fact are with respect to current run (from common dimensions) and previous run (from previous run dimension) combination and also the time dimensions of Time Day - Previous Run Date and Time (from common dimensions).

Subject Area – SOD Policy

The SOD Policy subject area has the following structure.

- **Policy Dimension:** Policy is defined from a group of entitlements and access points in combination. The Policy dimension is used with other dimensions and facts in the current folder.

- **Access Point:** The access point dimension is used with other dimensions and facts in the current folder.

- **Entitlement:** The entitlement dimension is used with other dimensions and facts in the current folder.

- **Instance:** The instance dimension is used with other dimensions and facts in the current folder.

- **Time Day - Policy Date:** This is the role playing version of the time dimension and can be used with other dimensions and facts in the current folder.

- **Fact - SOD Policy:** The SOD Policy fact has measures derived around all the dimensions in this subject area.

Subject Area – SOD Policy Conditions

The SOD Policy Conditions subject area has the following structure.

- Common Dimensions (refer to the Common Dimensions section of this chapter.)

- Conditions

- Path conditions

Conditions

- **Fact - SOD Conditions**

  - Condition Value - That holds value of the exclusions of type users, access point, SOB, OU etc.

  - Condition Value Status- The status mentions if the excluded value is Active, Inactive or NA

  - Condition Type – The condition type explains the type of condition. The type may be Users, Access Point, SOB etc

  - Condition Type Description – This attribute explains the description of condition types.

  - Condition Type Status - This status explains if the condition type is Active, Inactive or NA

  - Policy Count – The number of polices that are associated for this Condition (Type/Value)

  - Access Point Count - The number of access points that are associated for this Condition (Type/Value)

- Application User Count - The number of users that are associated for this Condition (Type/Value)

- Condition Value Effective Start Date- This is the start date for the Exclusion

- Condition Value End Date- This is the end date for the Exclusion

- Conditions Count – The number of exclusions.

- Global Condition Flag – This flag indicates whether exclusion type is excluded at global level or not.

- Policy Same Flag- This flag shows the value of same flag at policy level for an exclusion type. If Policy same flag is 'Yes' then this exclusion is associated with policy.

- Global Condition Value Flag- This flag indicates whether exclusion is excluded at global level or not.

- Global Same Flag- This flag shows the value of same flag at global level for an exclusion type.

- **SOD Condition Type**
  - Exclusion Type Effective Start Date- Exclusion type start date

  - Exclusion Type Effective End Date-Exclusion type end date

  - Condition Type-Exclusion type

  - Condition Type Id-Identifier for a particular exclusion type

  - Condition Type Description-Description for particular exclusion

  - Condition Type Code-Code value for exclusion type

  - Condition Type Status- This status explains if the condition type is Active, Inactive or NA Condition Type Status Code-Code for Condition Type Status

- **SOD Condition Value**
  - Condition Value- Value of Exclusion

  - Condition Value Status-This status explains if the condition value (exclusion value) is Active, Inactive or NA.

  - Condition Value Effective Start Date-Exclusion value start date

- Condition Value Effective End Date-Exclusion value end date

- Condition Value Status Code-Code value for Condition value status

- Condition Value Id-Identifier for Condition value

Path Conditions

- **Access Point Path Conditions**
  - Access Point Description- It explains description of access point which is excluded
  - Access Point Start Date- Start date of Access point which is excluded.
  - Access Point End Date- End date of Access point which is excluded.
  - Access Point Name- It shows Access point name which is excluded
  - Access Point Type- It shows the type of access point which is excluded

- **Access Point**
  - Access Point Name-It shows Access point name.
  - Access Point Type-It shows the type of access point.
  - Access Point Description-It explains description of access point.
  - Access Point Start Date-Start date of Access point.
  - Access Point End Date-End date of Access point.
  - Access Point Code-Code of Access point.
  - Access Point Type Code-Code of Access point type.

- **Access Point – From**
  - Access Point Name – From- It shows Access point name from which it is excluded
  - Access Point Description – From- explains description of access point from which it is excluded
  - Access Point Type – From- It shows the type of access point from which it is excluded

- Access Point Start Date – From- Start date of Access point from which it is excluded

- Access Point End Date – From- End date of Access point from which it is excluded

- Access Point Id – From- Identifier of Access point from which it is excluded.

- Access Point Code – From- Code of Access point from which it is excluded

- Access Point Type Code – From- of Access point type from which it is excluded

- **Application User – From**
  - Global User Name-If user is having existence in more than one application then his unique id/name across all the applications is known as global user name.

  - Related User Name-User's name in a particular application.

  - Related User Id-Identifier for User in the application.

  - Display Name-Name to be displayed in that application.

  - First Name-First name of User in application.

  - Last Name-Last name of user in an application.

  - User Status-This status indicates whether user is active or inactive.

  - User Description- Description of user in an application.

  - Email Address-E-mail address of the user.

  - Employee Id-Employee identifier for user.

  - User Start Date-Start date of user in that application.

  - User End Date-End date of the user in an application.

  - User Effective Start Date - SCD type2 attribute.

  - User Effective End Date - SCD type2 attribute.

- **Fact - SOD Path Conditions**
  - Condition Path Start Date- Start date for path of Exclusion.

  - Condition Path End Date-End date for path of exclusion.

- Condition Path Action-Action for Exclusion.(whether to exclude or not).

- Condition Path Status- this status indicates whether exclusion is active or inactive.

- Access Point Name-Name of Access point which is excluded.

- Access Point Type-Type of Access point which is excluded.

- Access Point Name – From-Name of access point from which it is excluded.

- Access Point Type – From-Type of access point from which it is excluded.

- Instance Name-Name of the instance for which exclusion is there.

- Instance Description-Description of Instance for which exclusion is there.

Metrics

Global User Conflict

Metric	Definition
SOD Policy Count	The count of SOD Policies
Total Conflict Count	This is the total count of SOD conflicts
Global User Count	This is the count of Global users
Run Count	This is the count of run
Month Ago Run Count	This is the count of run a month ago.
Year Ago Run Count	This is the count of run a year ago.
Number of Days Outstanding	The number of days that an SOD conflict has been identified but not resolved.
Approved Conflict Count	This is total the count of approved conflicts
Monitor Conflict Count	This is total the count of monitor conflicts

Pending Conflict Count	This is total the count of pending conflicts
Prevented Conflict Count	This is total the count of prevented conflicts
Rejected Conflict Count	This is total the count of rejected conflicts
Month Ago Total Conflict Count	This is the count of total conflicts a month ago.
Month Ago Approved Conflict Count	This is the count of approved conflicts a month ago.
Month Ago Monitor Conflict Count	This is the count of monitor conflicts a month ago.
Month Ago Pending Conflict Count	This is the count of pending conflicts a month ago.
Month Ago Prevented Conflict Count	This is the count of prevented conflicts a month ago.
Month Ago Rejected Conflict Count	This is the count of rejected conflicts a month ago.
Quarter Ago Total Conflict Count	This is the count of total conflicts quarter ago.
Quarter Ago Approved Conflict Count	This is the count of approved conflicts quarter ago.
Quarter Ago Monitor Conflict Count	This is the count of monitor conflicts quarter ago.
Quarter Ago Pending Conflict Count	This is the count of pending conflicts quarter ago.
Quarter Ago Prevented Conflict Count	This is the count of prevented conflicts quarter ago.
Quarter Ago Rejected Conflict Count	This is the count of rejected conflicts quarter ago.
Year Ago Total Conflict Count	This is the count of total conflicts a year ago.
Year Ago Approved Conflict Count	This is the count of approved conflicts a year ago.
Year Ago Monitor Conflict Count	This is the count of monitor conflicts a year ago.
Year Ago Pending Conflict Count	This is the count of pending conflicts a year ago.
Year Ago Prevented Conflict Count	This is the count of prevented conflicts a year ago.

Year Ago Rejected Conflict Count	This is the count of rejected conflicts a year ago.

Conflict Metrics

Metric	Definition
SOD Policy Count	The count of SOD Policies
Total Conflict Path Count	The count of total Conflict paths.
Entitlement Count	The count of entitlements.
Application User Count	The count of Application User.
Run Count	The count of runs.
Month Ago Run Count	The count of runs a month ago.
Year Ago Run Count	The count of runs a year ago.
Number of Days Outstanding	The number of days that an SOD conflict has been identified but not resolved.
Role Count	The count of roles.
Privilege Count	The count of privileges.
Assigned To User Count	The count of assigned to users.
Approved Conflict Path Count	The count of approved conflict paths.
Monitor Conflict Path Count	The count of Monitor conflict paths.
Pending Conflict Path Count	The count of Pending conflict paths.
Prevented Conflict Path Count	The count of Prevented conflict paths.
Rejected Conflict Path Count	The count of Rejected conflict paths.
Month Ago Total Conflict Path Count	The count of total conflict paths a month ago.

Month Ago Approved Conflict Path Count	The count of Approved conflict paths a month ago.
Month Ago Monitor Conflict Path Count	The count of Monitor conflict paths a month ago.
Month Ago Pending Conflict Path Count	The count of Pending conflict path a month ago.
Month Ago Prevented Conflict Path Count	The count of Prevented conflict paths a month ago.
Month Ago Rejected Conflict Path Count	The count of Rejected conflict paths a month ago.
Quarter Ago Total Conflict Path Count	The count of total conflict path paths a quarter ago.
Quarter Ago Approved Conflict Path Count	The count of total conflict path a quarter ago.
Quarter Ago Monitor Conflict Path Count	The count of Monitor conflict paths a quarter ago.
Quarter Ago Pending Conflict Path Count	The count of Pending conflict paths a quarter ago.
Quarter Ago Prevented Conflict Path Count	The count of Prevented conflict paths a quarter ago.
Quarter Ago Rejected Conflict Path Count	The count of Rejected conflict paths a quarter ago.
Year Ago Total Conflict Path Count	The count of total conflict paths a year ago.
Year Ago Approved Conflict Path Count	The count of Approved conflict paths a year ago.
Year Ago Monitor Conflict Path Count	The count of Monitor conflict paths a year ago.
Year Ago Pending Conflict Path Count	The count of Pending conflict paths a year ago.
Year Ago Prevented Conflict Path Count	The count of Prevented conflict paths a year ago.

Year Ago Rejected Conflict Path Count	The count of Rejected conflict paths a year ago.
Conflict Count	This is a distinct count of user surrogate key and policy surrogate key.

Policy Previous Run Metrics

Metric	Definition
Approved Conflict Path Count	The count of Approved conflict paths for the current run.
Monitor Conflict Path Count	The count of Monitor conflict paths for the current run.
Pending Conflict Path Count	The count of Pending conflict paths for the current run.
Prevented Conflict Path Count	The count of Prevented conflict paths for the current run.
Rejected Conflict Path Count	The count of Rejected conflict paths for the current run.
Total Conflict Count	This is the total conflicts for the current run.
Approved Conflict Count	This is the approved conflicts for the current run.
Monitor Conflict Count	This is the Monitor conflicts for the current run.
Pending Conflict Count	This is the Pending conflicts for the current run.
Prevented Conflict Count	This is the Prevented conflicts for the current run.
Rejected Conflict Count	This is the Rejected conflicts for the current run.
Total Conflict Path Count	This is the total conflict paths for the current run.
Previous Run Total Conflict Count	This is the count of total conflicts for previous run.
Previous Run Approved Conflict Count	This is the count of Approved conflicts for previous run.

Previous Run Monitor Conflict Count	This is the count of Monitor conflicts for previous run.
Previous Run Pending Conflict Count	This is the count of Pending conflicts for previous run.
Previous Run Prevented Conflict Count	This is the count of Prevented conflicts for previous run.
Previous Run Rejected Conflict Count	This is the count of Rejected conflicts for previous run.
Previous Run Total Conflict Path Count	This is the count of Total conflicts for previous run.
Previous Run Approved Conflict Path Count	This is the count of Approved conflict paths for previous run.
Previous Run Monitor Conflict Path Count	This is the count of Monitor conflict paths for previous run.
Previous Run Pending Conflict Path Count	This is the count of Pending conflict paths for previous run.
Previous Run Prevented Conflict Path Count	This is the count of Prevented conflict paths for previous run.
Previous Run Rejected Conflict Path Count	This is the count of Rejected conflict paths for previous run.
Latest Policy Run Flag	The flag indicates if a run is latest for a given Policy (Y/N) The flag is derived on Policy Id and the run surrogate key (not on Policy Surrogate Key).

SOD Policy Metrics

Metric	Definition
Total Policy Count	The total count of SOD Active Policies
Policy Count	The count of SOD active Policies
Entitlement Count	The count of Entitlement

Access Point Count	The count of Access Point
Instance Count	The count of Instance
Process Count	The count of Process
Risk Count	The count of Risk
Month Ago Policy Count	This is the count of policies a month ago.
Month Ago Entitlement Count	This is the count of Entitlement a month ago.
Month Ago Access Point Count	This is the count of Access Point a month ago.v
Month Ago Instance Count	This is the count of Instance a month ago.
Quarter Ago Policy Count	This is the count of policies a Quarter ago.
Quarter Ago Entitlement Count	This is the count of Entitlement a Quarter ago.
Quarter Ago Access Point Count	This is the count of Access Point a Quarter ago.
Quarter Ago Instance Count	This is the count of Instance a Quarter ago.
Year Ago Entitlement Count	This is the count of Entitlement a Year ago.
Year Ago Access Point Count	This is the count of Access Point a Year ago.
Year Ago Policy Count	This is the count of policies a Year ago.
Year Ago Instance Count	This is the count of Instance a Year ago.

SOD Conditions Metrics

Metric	Definition
Policy Count	The number of polices that are enforced with this Condition (Type/Value)

Access Point Count	The number of access points that participated with this Condition (Type/Value)
Application User Count	The number of users that participated with this Condition (Type/Value)
Conditions Count	This measure provides the number of Condition Types available that can be applied for a policy or set of policies.

Common SOD Dimensions

There is a common dimension folder in the following subject areas:

- Subject Area – SOD detail: The common dimensions are Policy, Run and Time

- Subject Area – SOD Conflicts: The common dimensions are Policy, Run and Time

- Subject Area – SOD Policy Conditions: The common dimensions are Policy, Run, Instance and Access Point

Using Common Dimensions

The common dimensions include Run, Policy and Time. These dimensions can be used across all the other folders. For example, you can use Policy dimension from Common dimensions folder with facts and dimensions in Conditions folder. You should only use the common dimensions with any one of the other folders. For example, you should not select dimensions from Common Dimensions, Conditions and also Path conditions. You should use dimensions from Common Dimensions and Conditions or dimensions from Common Dimensions and Path Conditions.

- **Policy Dimension:** Policy is defined from a group of entitlements and access points in combination. The Policy dimension is used with dimensions and facts from all the folders.

    - SOD user conflict specific analytics

    - SOD conflict path specific analytics

    - SOD Conflict Analytics by Run

    - SOD Conflicts

    - SOD Policy

- Conditions

- Path Conditions

- **Run Dimension:** The run dimension is used with dimensions and facts from all the folders. Do not use the run dimensions with folder SOD Policy.
  - SOD user conflict specific analytics

  - SOD conflict path specific analytics

  - SOD Conflict Analytics by Run

  - SOD Conflicts

  - Conditions

  - Path Conditions

- **Time Dimension:** The time dimension is used with dimensions and facts from all the folders.
  - SOD user conflict specific analytics

  - SOD conflict path specific analytics

  - SOD Conflict Analytics by Run

  - SOD Policy

  - Conditions

  - Path Conditions

SOD Conditions

AACG enforces conditions for a policy or a set of policies:

- **Policy level conditions** - The conditions are applied using the Same flag for the policies. This is the policy level conditions. The Same flag can hold values (Yes, No) to be set on the condition type for a policy.

- **Global level conditions** - Enforces a condition across all polices using the global condition as they are enforced on a given instance (EBS or Peoplesoft).

- **Global path conditions** - Enforces conditions at the path level. For example, we can set conditions for one access point with reference to another access point or user.

These are called global path conditions. Global conditions refer to conditions that are not based on a policy.

In GRI, you can report on condition that is set for a policy at:

- Condition Type level (For E.g. Access Point, User, SOB, OU etc)

- Condition Value level (For E.g. Values of Access Point, User, SOB, OU etc)

- Condition Paths (Apply condition on an Access point with respect to another access point or users)

Flags in the reports show how the conditions are applied in AACG:

- **Policy Same Flag** – In the reports we use this flag to indicate that the Same flag in the AACG application is applied for a policy with Condition type. If the Policy Same Flag is set to 'Yes' it means that for a policy, the same flag in AACG has value set to 'Yes' for the associated Condition type.

- **Global Same Flag** – In the reports we use this flag to indicate that the Same flag in the AACG application is applied for a Condition type that spans across all policies. We do not associate any single policy for the Condition type. If the Global Same Flag is set to 'Yes' it means that the same flag in AACG has value set to 'Yes' for the Condition type. This condition type is applied across all policies.

- **Global Condition Flag** – This flag indicates whether condition type is excluded at global level or not. In the reports, we use this flag to indicate that the Same flag in the AACG application is applied for a Condition type that spans across all policies. The difference between Global Same Flag and Global Condition Flag is that Global Same Flag contains value of same flag across all the polices while the Global Condition Flag mentions that If the condition type is excluded globally or not.

- **Global Condition Value Flag** - This flag indicates whether condition value is excluded at global level or not. In the reports, we use this flag to indicate that the Same flag in the AACG application is applied for a Condition value that spans across all policies.

Using Start and End Dates for Conditions

Using the start and end dates we capture when the Condition Value is applied for a policy or is removed from a policy, or again introduced for a policy. If a condition value/type is applied for a policy, the start date has the date when the condition was effective for a policy and end date has an infinite date. If the applied condition value/type is removed from the policy, then the end date is updated from infinite date to the date when the condition value/type is removed from the policy. Again, if the condition is applied for a policy, a new row is created with the start date has the date when the condition was effective for a policy and end date has an infinite date.

To see the dates in the reports use the following attributes:

- Condition Value Start Date

- Condition Value End Date

- Condition Type Start Date

- Condition Type End Date

Conditions Metrics

The following metrics are specific to the Conditions and Path conditions:

- Policy Count – The number of polices that are enforced with this Condition (Type/Value)

- Access Point Count - The number of access points that participated with this Condition (Type/Value)

- Application User Count - The number of users that participated with this Condition (Type/Value)

- Conditions Count – This measure provides the number of Condition Types available that can be applied for a policy or set of policies.

SOD Path Conditions

This is applicable at the access point level. Here the access point is excluded from another access point or user. All path conditions are set at the global level or instance level. The action is set to 'Excluded' this means that the access point is excluded from the related user or access point. The status is set to 'Active' or 'Inactive'. This means that the condition is 'Active' or 'Inactive'. The Condition Path Start Date and Condition Path End Date attributes explain when the path condition was set for an access point.

In AACG application, you can create global path conditions. Each excludes one access point from another, such as an Oracle function from a menu or a responsibility. A path including those points would be excluded from conflict generation. If, for example, a global path condition excluded function1 from responsibility1, an access policy set function1 in conflict with function2, and a user had access to both functions, no conflict would occur if the user's access to function1 came from responsibility1.

This information can be viewed in our reports by using the facts and dimension in the Path Conditions folder.

A

Modifying Reports and Dashboards

This appendix covers the following topics:

- Modifying Report Titles
- Creating Report Prompts
- Modifying Charts
- Creating Formulas within Reports
- Modifying Tables
- Modifying Pivot Tables
- Conditional Formatting
- Modifying Data Formats
- Using Filters
- Printer Friendly Reporting
- Supported Languages
- Modifying Dashboards

Modifying Report Titles

To modify a report title:

1. Select the Modify link on any report.

2. Select the Results tab.

3. From the drop down menu, choose Title.

4. You can edit the report title, subtitle or image.

5. Select the Save icon when you are finished making changes to your title.

Tips on Modifying Report Titles

- The name you give the report when you save it is the title that will be displayed when the report is executed.

- When saving your report, enter a description for the report. The description appears as a tooltip when you "hover" the mouse over the report title in Answers and on Dashboards.

- If your chart or table is drillable, add a subtitle such as "(Drill on chart for details)"

- If desired, set the 'Started Time' to 'Display date & time'. Note that this may not always be desirable and can clutter up the title.

- Adding an image to a report:
  - Image names are always prefixed with "fmap:Images/"

  - The image should appear to the left of the title.

To add an image to the report, find the image you wish to use in the following table, then enter that image's reference in the Logo field.

Image	Logo Field Entry "fmap:Images/___"	Image	Logo Field Entry "fmap:Images/___"
	fmap:Images/report_account_appl.jpg		fmap:Images/report_good_value.jpg
	fmap:Images/report_activities.jpg		fmap:Images/report_household.jpg
	fmap:Images/report_agreements.jpg		fmap:Images/report_insurance_Policy.jpg
	fmap:Images/report_automotive1.jpg		fmap:Images/report_insuranceClaim.jpg fmap:Images/report_tradefund.jpg
	fmap:Images/report_automotive2.jpg		fmap:Images/report_investigative.jpg
	fmap:Images/report_bad_percentage.jpg		fmap:Images/report_invoices.jpg
	fmap:Images/report_bad_progress.jpg fmap:Images/report_bottomN.jpg		fmap:Images/report_location.jpg
	fmap:Images/report_bad_value.jpg		fmap:Images/report_medicalResearch.jpg
	fmap:Images/report_bankAccount.jpg		fmap:Images/report_mktShare.jpg
	fmap:Images/report_bankBalances.jpg		fmap:Images/report_order.jpg
	fmap:Images/report_call.jpg		fmap:Images/report_phone.jpg
	fmap:Images/report_callcenter.jpg		fmap:Images/report_pillcount.jpg

	fmap:Images/report_cautionary_percentage.jpg		fmap:Images/report_pipeline.jpg
	fmap:Images/report_cautionary_progress.jpg		fmap:Images/report_reportsCatalog.jpg
	fmap:Images/report_cautionary_value.jpg		fmap:Images/report_retailAudit.jpg
	fmap:Images/report_comm1.jpg		fmap:Images/report_salesrep.jpg
	fmap:Images/report_comm2.jpg		fmap:Images/report_scorecard.jpg
	fmap:Images/report_cust_sat.jpg		fmap:Images/report_service_profitibility.jpg
	fmap:Images/report_email.jpg		fmap:Images/report_serviceRequest.jpg
	fmap:Images/report_expiration.jpg		fmap:Images/report_targetActual.jpg
	fmap:Images/report_forecasting.jpg		fmap:Images/report_tradepromo.jpg
	fmap:Images/report_generic.jpg fmap:Images/report_salesVolume.jpg		fmap:Images/report_trends.jpg
	fmap:Images/report_geographical.jpg		fmap:Images/report_universal_queue.jpg
	fmap:Images/report_good_percentage.jpg		fmap:Images/report_win_lossDeals.jpg
	fmap:Images/report_good_progress.jpg fmap:Images/report_topN.jpg		

Creating Report Prompts

Use prompts to obtain user input before showing the report. To create a report prompt:

1. Select the Modify link on any report.

2. Select the Prompts tab.

3. From the Create Prompt menu, choose one of the following:

   - Column Filter Prompt: A column filter prompt provides general filtering of a column within a request. A column filter prompt can present all choices for a column, or it can present constrained choices for a column. For example, if a request contains a Region=East filter, constraining choices for the City column restricts the selections to cities in the East region only. This eliminates the selection of a mutually exclusive filter that could result in no data.

Column Filter Prompt Properties

Caption

Description

Filter on Column   Risk Significance

Operator   is equal to / is in

How should the user choose a value or values?

⦿ Select it from a drop-down list

○ Browse through choices and/or type in directly

☑ Single Value Only

What values should be shown to the user?

○ None

⦿ All Values

○ Limited Values

○ SQL Results

(The values returned by this SQL statement)

Other options

Choices per page

(leave blank for automatic setting)

☐ Allow user to constrain choices

☐ Allow user to skip prompt

OK   Cancel

- Image Prompt: An image prompt provides an image that users click to select criteria for a request. For example, in a sales organization, users can click their territories from an image of a map to see sales information, or click a product image to see sales information about that product. Users who know how to use the HTML <map> tag can create an image map definition.

Image Map Prompt Properties

Caption

Description

Image URL

HTML Image Map

HTML

Extract Image Map from HTML

OK   Cancel

4. Select the Save icon when you are finished creating your report prompt.

Tips on Creating Report Prompts

- Prompts allow the user to provide input which filters large amounts of information in order to get meaningful output.

- Example of a Column Filter Prompt as it would appear in a report:

Week

Add Another Value

Week of 9/29/2003 – 10/5/2003
Week of 10/6/2003 – 10/12/2003
Week of 10/13/2003 – 10/19/2003
Week of 10/20/2003 – 10/26/2003
Week of 10/27/2003 – 11/2/2003
<< **1** >>

Go

Modifying Charts

To modify a chart:

1. Select the Modify link on any report.

2. Select the Results tab.

3. From the drop down menu, choose Chart.
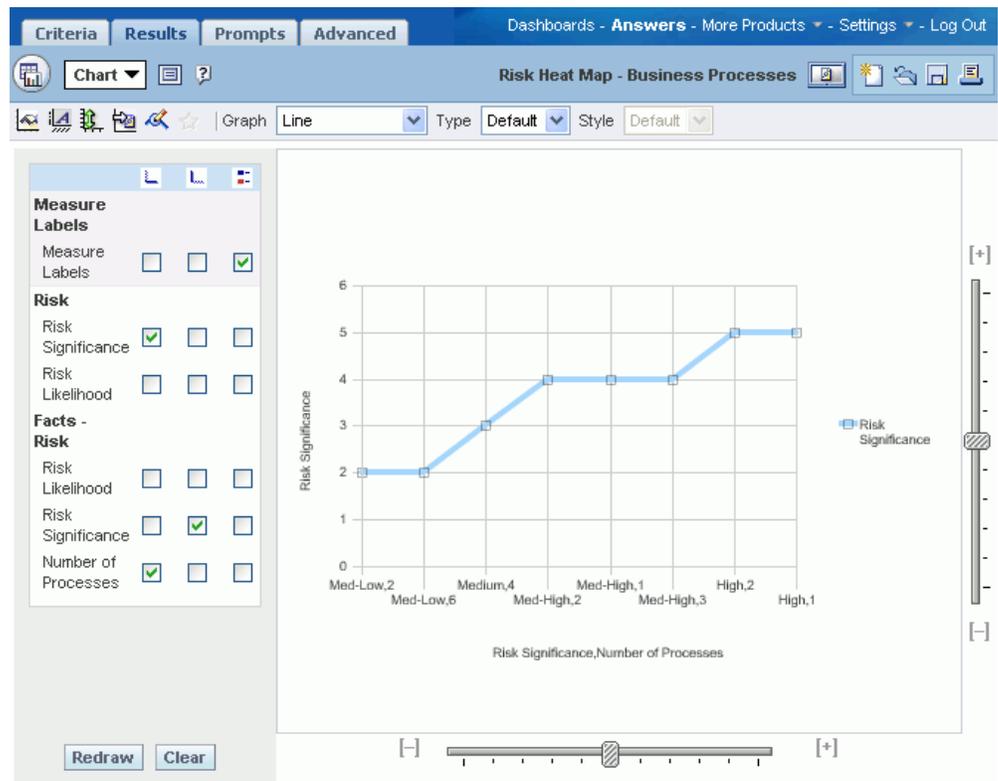
4. Make changes as appropriate.

5. Select the Save icon when you are finished making changes to your chart.

Tips on Modifying a Chart

- When creating a report that will show a chart, include only the columns that you need to render the chart. Columns included in the criteria but not shown are still run and aggregated, which can adversely affect performance.

- Leave the chart size as initially displayed. Generally, the chart should be the size needed to successfully achieve its purpose. It is okay if a summary chart is smaller than a detailed one. Charts of different sizes will also lend some visual interest to the page.

- In general, a light background color on a chart can add emphasis to the chart and visual interest to a page. For example:

chart test

The Worlds Greatest Chart Title

CHICAGO DISTRICT
CINCINNATI DISTRICT
DETROIT DISTRICT
KANSAS CITY DISTRICT
MINNEAPOLIS DISTRICT
BOSTON DISTRICT
NEW YORK DISTRICT
PHILADELPHIA DISTRICT
YOUNGSTOWN DISTRICT
ATLANTA DISTRICT
CHARLOTTE DISTRICT
DALLAS DISTRICT
JACKSONVILLE DISTRICT
MEMPHIS DISTRICT
DENVER DISTRICT
LOS ANGELES DISTRICT
PORTLAND DISTRICT
SAN FRANCISCO DISTRICT

4.55% 4.04%   6.51%
3.46%
4.24%
14.51%
3.01%
1.26%
8.62%
3.46%
1.76%
8.5%
11.93%
4.93%
1.05%
2.73%
9.94%
5.5%

- If displaying multiple charts in a report, enter a title for each chart for better usability.

- Place legends in the appropriate location for the chart type displayed. As horizontal space is usually the limiting dimension, a top or bottom location often works best. This should be applied consistently by page.

- Include axis titles where necessary.

- Try to mix use of different chart types, for example, Vertical Bar, Horizontal Bar, Line Bar Combo, and Pareto. Variety is good, but use the chart types which are best suited to illustrate different types of data. For example, use lines for trends, bars for comparison between series, stacked to show contributions to a whole.

- If using many Vertical Bar or Horizontal Bar graphs, try to mix use of different styles, such as Rectangle, Cylinder and Gradient.

- Make charts to further detail reports, but try to keep drilling to 2 levels (parent report to child report) to prevent confusing navigation.

- For gauges, use the default colors and gauge attributes:

Criteria | Results | Prompts | Advanced   Dashboa

Gauge ▼ 回 ?   Risk Mitigatio

☆ | Gauge Dial ∨ Type Default ∨ | Size Default ∨ | Clear
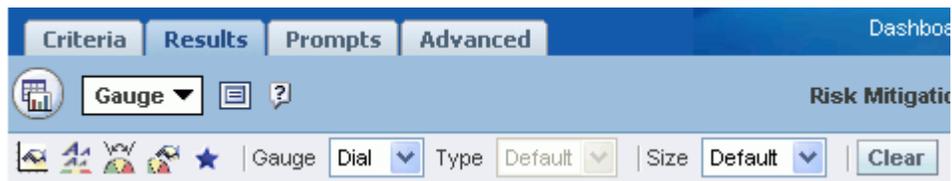
- For Line Graphs or Line Bar Combo Graphs, turn off line symbols:
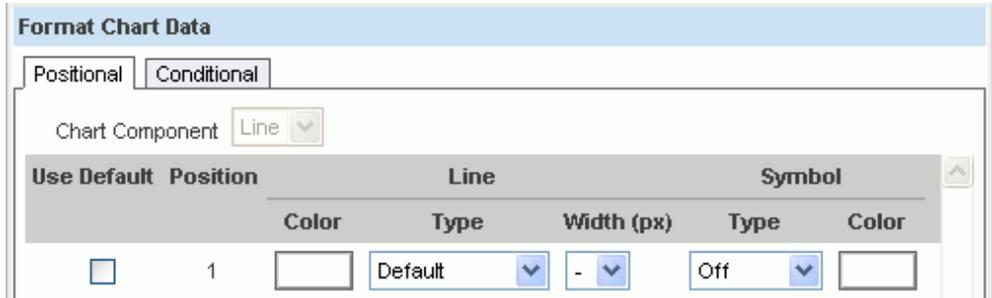
Creating Formulas within Reports

Avoid creating new formulas within reports (for example, CASE statements or calculations), instead, define formulas as metrics. This prevents the need to recreate metrics that can be reused in other reports.

Modifying Tables

To modify a table:

1. Select the Modify link on any report.

2. Select the Results tab.

3. From the drop down menu, choose Table.

4. Make changes as appropriate.

5. Select the Save icon when you are finished making changes to your table.

Tips on Modifying Tables

- When creating a report, always place the parent attribute in the left-outer-most column followed by the respective children in hierarchical order.

- If an Enterprise Analytics Applications has Logical Column Names that are identical within the same Subject Area, rename and prefix both columns so end-users can differentiate between the two columns (for example, Finished Goods Product Name and BOM Product Name).

- For large tables with many columns and rows, use bar shading to make the table more readable. Note, however, that in some cases, the addition of the shaded bar format will render a table less usable if the grouping with the value suppression option is turned off.

- Left-justify labels if displaying labels in a column.

- Change the number of records displayed to vary the height of a table. The default is 25 rows per page.

- Select the Table View Properties button to enable column sorting in Dashboards. Column sorting in Dashboards works best when there is a small set of records (fewer than 100) in an analysis.

Modifying Pivot Tables

To modify a Pivot table:

1. Select the Modify link on any report.

2. Select the Results tab.

3. From the drop down menu, choose Pivot Table.

4. Make changes as appropriate.

5. Select the Save icon when you are finished making changes to your pivot table.

Tips on Modifying Pivot Tables

- When creating the criteria for a pivot table, only include the columns that you absolutely require to render the pivot table.

- Conditional formatting is carried over to pivot tables except for conditional formatting based on another column. Conditions must be based on the column to which they apply.

- Use the pivot table functionality to create "% of total" columns where needed.

- Make creative use of pivot tables. Create mini pivot tables as summary tables on top of a report.

Conditional Formatting

To add conditional formatting to a table:

1. Select the Modify link on any report.

2. Select the Results tab.

3. From the drop down menu, choose Table.

4. Select the Column Properties button.
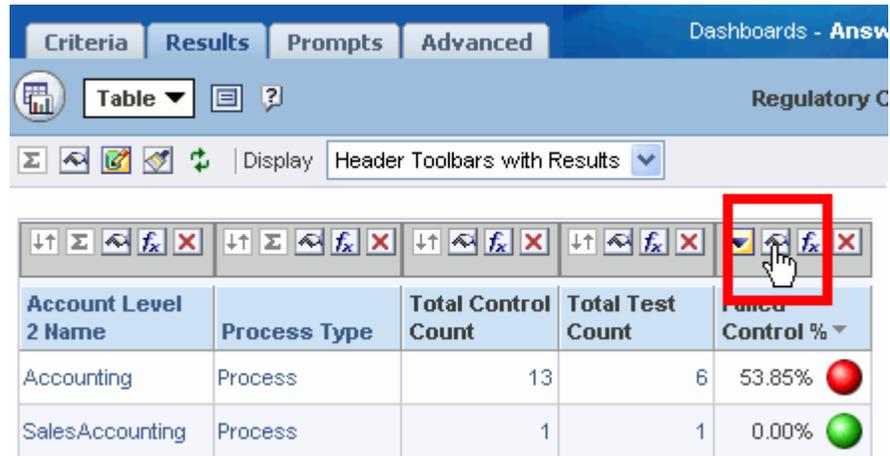
5. Make changes as appropriate on the Conditional Format tab. Refer to the online help for details.

6. Select the Save icon when you are finished making changes.

Tips on Conditional Formatting

- If you use graphics, remember to use the "null" images for the conditions that are not met, so alignment of text and numbers is preserved. In the following example, when there are no failed controls, a green circle is displayed, which keeps the column properly aligned.

- Display legends to explain the conditional formatting using the Legend option.

- Conditional formatting allows conditions on other columns in your report, not just the column with the formatting. For example, if you are doing comparisons with historical data, you can try using the red down arrows and blue up arrows to indicate trends.

Modifying Data Formats

To modify data formats in a table:

1. Select the Modify link on any report.

2. Select the Results tab.

3. From the drop down menu, choose Table.

4. Select the Column Properties button.

5. Make changes as appropriate on the Data Format tab. Refer to the online help for details.

6. **Important:** When you select the Save button, make sure that you save as the system-wide default for your specific metric. Do not save as the system-wide default for this data type; this can cause formatting of other metrics to change and can cause a lot of rework. For example:
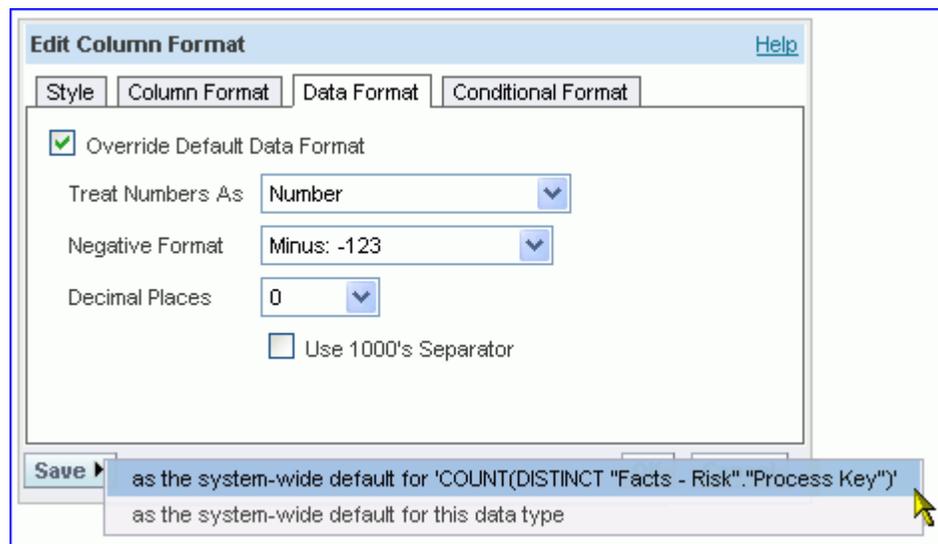
Using Filters

To add a filter to a report:

1. Select the Modify link on any report.

2. Select the Critera tab.

3. To add a new filter, select the Filter button for the appropriate column.
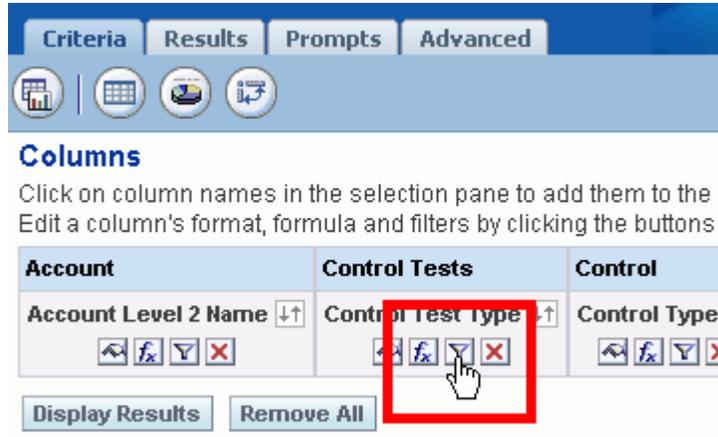
4. Make changes as appropriate.

5. Select Ok when you are done making changes, then save your work.

Tips on Using Filters

- For dynamic data, analyses should only contain "Is Prompted" filters (that is, nothing should be hard-coded).

- Saved filters should be used when you wish to filter a lot of reports by a set number of filtered columns. For example, if you wish to filter to the current year, create then reference a Shared Filter called "Current Year" instead of Year = 2008, or create a Shared Filter called "Current Year Prompted" instead of Year is prompted.

- Try to include column selectors in your reports. Add labels for column filters, such as "Select View". For example:

Controls Count - Summary

Select Dimension: Account Level 2 Name   Select Metric: Key Control Count

- To use repository variables in your filters, select Add -> Variable in the Create/Edit Filter screen, then enter the variable name. The following is a list of repository variables that you can use in your filters:

    - CURRENT_DAY

    - CURRENT_FSCL_MONTH

    - CURRENT_FSCL_QUARTER

    - CURRENT_FSCL_YEAR

    - CURRENT_FSCL_WEEK

    - CURRENT_JULIAN_DAY_NUM

    - CURRENT_MONTH

    - CURRENT_QUARTER

    - CURRENT_YEAR

    - CURRENT_WEEK

    - LAST_REFRESH_DT

    - NEXT_FSCL_MONTH

    - NEXT_FSCL_QUARTER

    - NEXT_FSCL_YEAR

    - NEXT_FSCL_WEEK

    - NEXT_MONTH

    - NEXT_QUARTER

    - NEXT_YEAR

    - NEXT_WEEK

- PREVIOUS_FSCL_MONTH

- PREVIOUS_FSCL_QUARTER

- PREVIOUS_FSCL_YEAR

- PREVIOUS_FSCL_WEEK

- PREVIOUS_MONTH

- PREVIOUS_QUARTER

- PREVIOUS_YEAR

- PREVIOUS_WEEK

Printer Friendly Reporting

Add Global Header and Footer to reports that you expect a user to print. To add a header and footer:

1. Select the Modify link on any report.

2. Select the PDF and Print Control button.
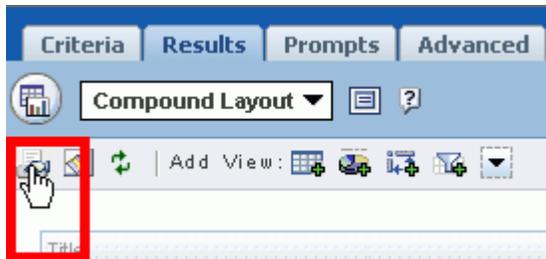
3. Select the Include Header and/or Include Footer check boxes.

4. Select the Edit button to specify how you want the header or footer to appear.

PDF and Print Control

Page Settings

Paper Size User Default

Orientation Portrait

Print Rows Visible

Header and Footer

☑ Include Header Edit

☑ Include Footer Edit

OK   Cancel

5. Select the Save icon when you are finished making changes.

Supported Languages

GRC Manager supports multiple languages in the user interface, where a user can override the default language through User Preferences. The languages delivered with GRC Manager include:

- Chinese Standard (zh)

- Chinese Traditional (zh_tw)

- Danish (da)

- French (fr)

- German (de)

- Italian (it)

- Japanese (ja)

- Korean (ko)

- Portuguese Brazilian (pt_br)

- Spanish (es)

The administrator has the ability to change the display text by language, which is modified via Administrative Tools.

Modifying Dashboards

To modify a dashboard, select Edit Dashboard from the Page Options menu. When modifying a dashboard, keep the following suggestions in mind:

- On a Dashboard page with multiple columns and rows, summarized analyses are typically shown first. End-users should be able to quickly view a summarized analysis, uncover a problem or opportunity and drill-down into details.

- Try not to place too many reports per dashboard. Remember that performance will suffer if there are a large number of reports embedded within a dashboard.

- Try to make dashboards look symmetric both vertically and horizontally. For example, fill available space, but leave some white space between content.

- To provide variety in Dashboard layout, use the "Insert Column Break" function on a column to obtain spanning columns. Or, use the "Horizontal Alignment" option for a section; this distributes a section's content horizontally as opposed to vertically.

- Enter descriptions for dashboards and pages. Descriptions appear as tooltips when you hover the mouse over the dashboard links in the top banner and page tabs.

- Remember to add links to Modify, Refresh, Download and Print to your reports.

Index