

**Oracle® Fusion Governance, Risk and Compliance
Intelligence**

Implementation Guide

Release 2.0

Part No. E10891-03

October 2008

Oracle Fusion Governance, Risk and Compliance Intelligence Implementation Guide, Release 2.0

Part No. E10891-03

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

Primary Author: Douglas J. Myers

Contributing Author: Anitha Raghavan, Ashwin Sadanandan, B'far Reza, Chandramoham Subbiah, Denise Fairbanks Simpson, Hal Kazi, Hernan Capdevila, Hugh Mason, Kim Wilmot, Louis Gonzales, Madhavi Gopaladasu, Mohamed Hussain, Mumu Pande, Pamela Rietz, Pournima Patil, Prasanna Chimata, Sinha Siddharth, Srinivasan Ganesan

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

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS

Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications which may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

This software and documentation may provide access to or information on content, products and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third party content, products and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third party content, products or services.

Contents

Send Us Your Comments

Preface

1 About Oracle Fusion Governance, Risk and Compliance Intelligence

Product Overview.....	1-1
About This Guide.....	1-3
Supported Languages.....	1-3
Prerequisites.....	1-4
Recommendation.....	1-4

2 Installing Oracle Fusion Governance, Risk and Compliance Intelligence for GRCM 7.8

Overview.....	2-1
Installing Oracle GRCM Scripts.....	2-1
Setting Up the Environment.....	2-2
Creating the Target Physical Model.....	2-17
Loading Target Tables.....	2-17
Installing OBIEE Reports.....	2-18
Multi-Language Setup for OBIEE.....	2-19
Installing BI Publisher Reports.....	2-24
Security Integration with GRCM (Optional).....	2-28

3 Installing Oracle Fusion Governance, Risk and Compliance Intelligence for AACG 8.1.1 or Later

Overview.....	3-1
---------------	-----

Installing Oracle AACG Scripts.....	3-1
Installing ODI Code.....	3-2
Installing OBIEE Reports.....	3-12
Security Integration with AACG (Optional).....	3-13

4 Installation and Upgrade Options for Oracle Fusion Governance, Risk and Compliance Intelligence 2.0

Overview.....	4-1
Installing Oracle Fusion Governance, Risk and Compliance Intelligence for both GRCM 7.8 and AACG 8.1.1 or Later.....	4-1
Upgrading GRCI 1.0 to GRCI 2.0.....	4-2

A ETL Execution

Execution Sequence.....	A-1
ETL Execution.....	A-2
Execute a Package.....	A-3

B Architecture

Data Flow Diagram.....	B-1
Detailed Data Flow Diagram.....	B-3

C Logical and Physical Models

Data Flow Diagram.....	C-1
GRCI - AACG 8.1.1 or later Logical Model.....	C-1
GRCI - AACG 8.1.1 or later Physical Model.....	C-5
GRCI - GRCM 7.8 Logical Model.....	C-19
GRCI - GRCM 7.8 Physical Model.....	C-21

D Lineage for GRCM 7.8

GRCI 2.0 - GRCM 7.8 Data Lineage CONSTANTS Table.....	D-1
GRCI 2.0 - GRCM 7.8 Data Lineage DIMENSIONS Table.....	D-5
GRCI 2.0 - GRCM 7.8 Data Lineage FACTS Table.....	D-10

E Lineage for AACG 8.1.1 or Later

GRCI 2.0 - AACG 8.1.1 or Later, Data Lineage DIMENSIONS Table.....	E-1
GRCI 2.0 - AACG 8.1.1 or Later, Data Lineage FACTS Table.....	E-4

Index

Send Us Your Comments

Oracle Fusion Governance, Risk and Compliance Intelligence Implementation Guide, Release 2.0 Part No. E10891-03

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 Oracle MetaLink 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 of the *Oracle Fusion Governance, Risk and Compliance Intelligence Implementation Guide*.

Oracle Fusion Governance, Risk and Compliance Intelligence Implementation Guide for Release 2.0 is intended for information technology personnel and privileged users responsible for installing and configuring the GRC Intelligence application. It assumes the reader is familiar with Oracle Content Server installation, configuration, and use.

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

TTY Relay Access to Oracle Support Services

To reach AT&T Customer Assistants, dial 711 or 1.800.855.2880. An AT&T Customer Assistant will relay information between the customer and Oracle Support Services at 1.800.223.1711. Complete instructions for using the AT&T relay services are available at <http://www.consumer.att.com/relay/tty/standard2.html>. After the AT&T Customer Assistant contacts Oracle Support Services, an Oracle Support Services engineer will handle technical issues and provide customer support according to the Oracle service request process.

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 About Oracle Fusion Governance, Risk and Compliance Intelligence**
- 2 Installing Oracle Fusion Governance, Risk and Compliance Intelligence for GRCM 7.8**
- 3 Installing Oracle Fusion Governance, Risk and Compliance Intelligence for AACG 8.1.1 or Later**
- 4 Installation and Upgrade Options for Oracle Fusion Governance, Risk and Compliance Intelligence 2.0**
- A ETL Execution**
- B Architecture**
- C Logical and Physical Models**
- D Lineage for GRCM 7.8**
- E Lineage for AACG 8.1.1 or Later**

Related Information Sources

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

This guide provides information on how to use the Governance, Risk and Compliance Intelligence application with Oracle Content Server.

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.

About Oracle Fusion Governance, Risk and Compliance Intelligence

Product Overview

Oracle Fusion Governance, Risk and Compliance Intelligence (GRCI), Release 2.0, is an intelligence reporting application that extracts data from Oracle Governance, Risk and Compliance Manager (GRCM), Release 7.8 and Oracle Application Access Control Governor (AACG) 8.1.1.

The Oracle Fusion Governance, Risk and Compliance Intelligence solution is designed to enhance your visibility into the organization's compliance readiness and responsiveness by providing certification, controls, issues, risks, and testing diagnostics and out-of-the-box management reports. By using Oracle Fusion Governance, Risk and Compliance Intelligence, you can drill from high-level to detailed information to effectively plan, model, report, and analyze GRC activities. You can identify potential issues early and take informed and timely corrective actions.

GRCI Sourced from AACG

- **GRCI Analytics Integration Overview** The source of GRCI Release 2.0 data store is AACG (Application Access Control Governor) 8.1.1 and information such as policies, entitlements, exclusions, conflicts etc., are loaded into GRCI staging tables hosted in the GRCI (data store) schema. This data load is accomplished in a 'push' fashion as opposed to the traditional 'extract' method and it is called Analytics Integration. Two enhancements were made to the AACG application to integrate with GRCI:
 1. A new tab called 'Analytics Integration' which is available through the Application Configuration screen. This captures the setup information related to the integration.
 2. Conflict run in AACG 8.1.1 or later is enriched with 'AACG data services' to load data into GRCI staging tables.

The other source of GRCI is GRM 7.8 and information such as Processes, Controls, Risks, Issues etc., from GRM 7.8 are loaded into GRCI data store tables for analysis using SQL.

- **Analytics Integration Schemas** The analytics integration component of AACG application uses two schemas to create necessary data for analysis by GRCI application. One schema (referred to as ag_access) stores AACG specific data in tables prefixed with LAA_ and TMP_ and another schema (referred to as gri) contains the staging tables used by GRCI ETL process. This gri schema contains all database objects used by the GRCI application.
- **Staging Tables Load** The gri schema contains the staging tables (prefixed with GRI_S_), which act as an interface between AACG and GRCI applications. These tables are populated when the user executes the Conflict Run process in AACG application.

Note: Check the AACG documentation for details on how to configure the application to connect to GRCI staging schema and load data into these staging tables.

The staging (GRI_S_) tables are loaded during every execution of Conflict Run and data is updated in the staging tables in an update-else-insert fashion. Here are two examples:

1. If the entitlement description or entitlement status changes in AACG, the AACG data services component will pick up the changes during the next Conflict Run, and update the staging tables GRI_S_ENTITLEMENT and GRI_S_ENTITLEMENT_TL with the new values.
 2. If the status of a Conflict Path changes from Approved to Rejected in AACG, the AACG data services component will pick up the changes during the next Conflict Run and update the staging table GRI_S_CONFLICT_PATH.
- **GRCI Star Schema Tables Load** Data in the GRCI staging schema is refreshed during every execution of Conflict Run in AACG. So as a best practice it is recommended that GRCI administrator execute the ODI based ETL packages immediately after every successful execution of Conflict Run (for ex: Run-1) in AACG. This would refresh the content of GRCI star schema tables and users can visualize the latest values in OBIEE based dashboards and reports. If the ETL packages are not executed before the next Conflict Run (for ex: Run-2) in AACG, the data in GRCI staging tables will be overwritten before the previous Run's (Run-1) changes being propagated to GRCI star schema tables.

GRCI Sourced from GRM GRM 7.8 is one of the sources of GRCI 2.0, and information such as Processes, Controls, Significant Accounts, Risks and Issues are extracted from GRM and loaded into the GRCI data store. The creation of the GRCI

Star Schema, Extraction, Transformation and Load of GRCM data into the GRCI star schema is accomplished using PL/SQL scripts. For further details on implementing GRCM based GRCI, please refer to Chapter 2.

About This Guide

This document explains how to install the Oracle Fusion Governance, Risk and Compliance Intelligence application on a Oracle 10g server. The information contained in this document is subject to change as the product technology evolves and as hardware, operating systems, and third-party software are created and modified. This document is intended for information technology personnel and authorized users responsible for installing and configuring the Oracle Fusion Governance, Risk and Compliance Intelligence, Release 2.0 application.

Supported Languages

Oracle Fusion Governance, Risk and Compliance Intelligence, Release 2.0 is available in English only for AACG 8.1.1 or later.

About Language Resource Files

GRCM 7.8 supports the following languages aligned with the Oracle Identity Management (OIM) product line:

- Chinese Traditional
- Chinese Standard
- Spanish
- French
- Japanese
- Portuguese
- Korean
- German
- Italian
- Danish
- Dutch
- UK English

Prerequisites

Before you use Oracle Fusion Governance, Risk and Compliance Intelligence, Release 2.0, you must:

- Install Oracle Database 10gR2 with patch 10.2.0.4
 - Install Oracle Business Intelligence Enterprise Edition 10.1.3.3.3
- Install either one or both of the following applications:
- Oracle Governance, Risk and Compliance Manager, Release 7.8
 - Install Oracle Application Access Control Governor 8.1.1
 - Install Oracle Data Integrator 10.1.3

If you have installed Oracle Application Access Control Governor 8.1.1, then:

- Install Oracle Data Integrator 10.1.3
- AACG Interface tables (tables with name starting as GRI_S_...) should be deployed in the same schema as the tables for data warehouse ('GRI' Schema).

Recommendation

It is recommended that the AACG installation and the data warehouse database that has 'GRI' schema (AACG DB and GRCI DB) be in the same network.

Installing Oracle Fusion Governance, Risk and Compliance Intelligence for GRCM 7.8

Overview

This chapter covers the installation procedures for GRCI 2.0 when the source application is solely GRCM 7.8. However, if there is an existing GRCI 1.0 installation, which needs to be upgraded to GRCI 2.0, please refer to Chapter 4, and follow the upgrade instructions.

Installing Oracle Scripts contains the following subsections:

1. Setting Up the Environment
2. Creating the Target Physical Model
3. Loading Target Tables

Installing Oracle GRCM Scripts

The GRI_20_GRCM_ETL.zip contains the scripts for the creation of the GRCI 2.0 datastore based on GRCM 7.8. When the scripts are executed as per the steps mentioned in this section, the GRCI star schema is created and loaded with the data from the source. With this release GRCI datastore can only be hosted on Oracle, but GRCM residing on SQLServer or Oracle database platforms can be used as the source.

The extracted zip file contains the following files:

- Model/Constants_Create_pkg.sql
- Model/Dims_Create_pkg.sql
- Model/Facts_Create_pkg.sql

- Model/Stage_Create_pkg.sql
- Model/Execute_Create.sql
- Model/Execute_Index_View.sql
- ETL/Constants_Load_pkg.sql
- ETL/Dims_Load_pkg.sql
- ETL/Facts_Load_pkg.sql
- ETL/ Execute_Load.sql

Important: If you are installing GRC Intelligence Release 2.0 for GRC Manager and AACG, then AACG Scripts Installation should be completed first, followed by the GRC Manager Scripts Installation.

Setting Up the Environment

1. Identify the source application database details - host name, port number, user name, and password.
2. Connect to source database depending upon the type of source: If the source is ORACLE: Connect to target oracle database using any oracle db connectivity client (e.g. SQL Developer). Create a database link - GRM771_APPS_DBLINK pointing to source database as follows. Replace the contents in <> brackets with the information in Step1 for creating the db link.
3. `CREATE DATABASE LINK GRM771_APPS_DBLINK CONNECT TO "<user name>" IDENTIFIED BY "<password>" USING DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST= <host name> or IP Address>)(PORT=<port name>)))(CONNECT_DATA (SERVICE_NAME=<service name>)))`

Verify if the database link is working by querying a source table. Refer below for an example.

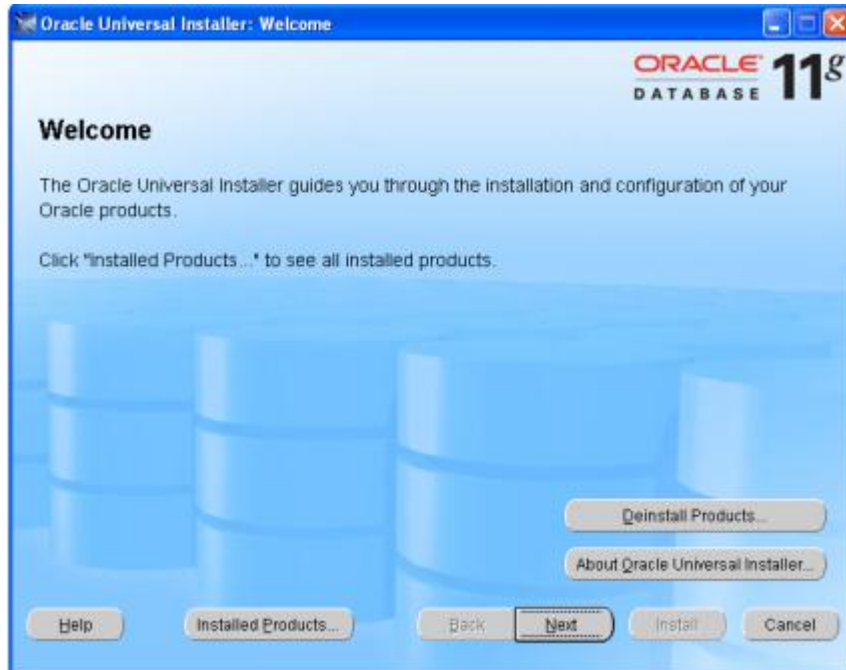
```
SELECT COUNT (*) FROM GRC_FISCAL_PERIODS@ GRM771_APPS_DBLINK;
```

If the source is SQL server: For connecting to the SQL server, the Oracle Database Gateways 11g Release 1 (11.1.0.6.0), should be installed in the oracle home directory of the database. All versions of gateway before this have been de-supported by Oracle and cannot be used.

For the Oracle database, a patch should be applied to upgrade it to 10.2.0.4, as the older versions of Oracle do not support the Unicode data transfer.

Follow this procedure to install the gateways in a windows Oracle database:

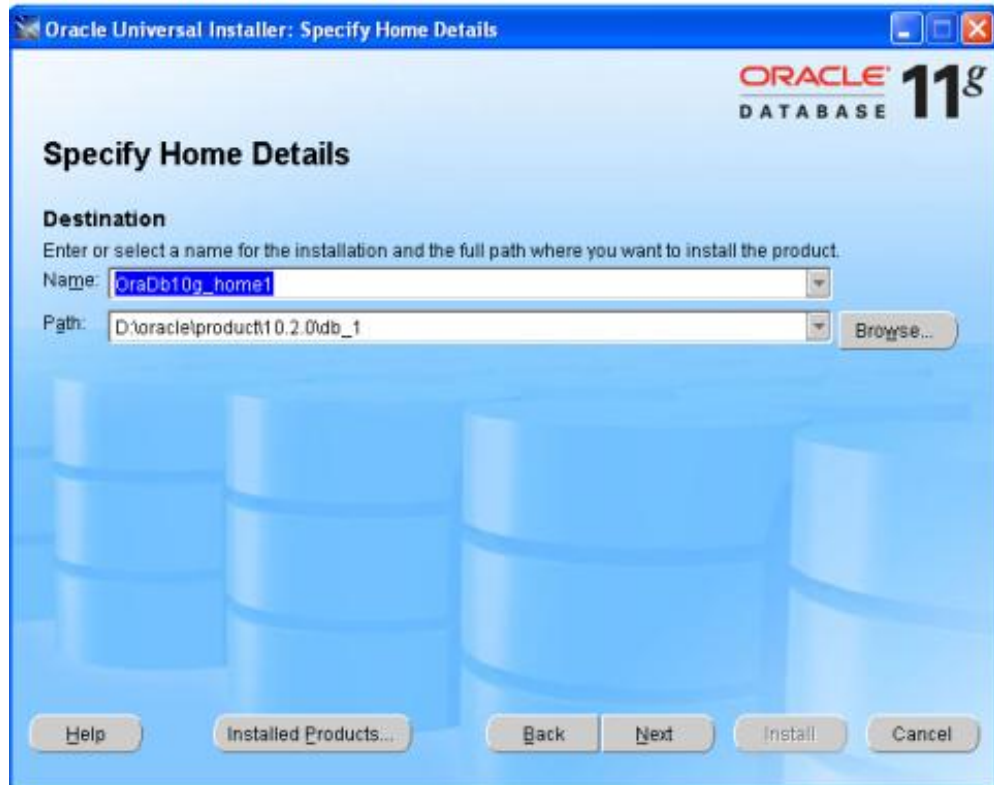
- Run the setup.exe from the install files.



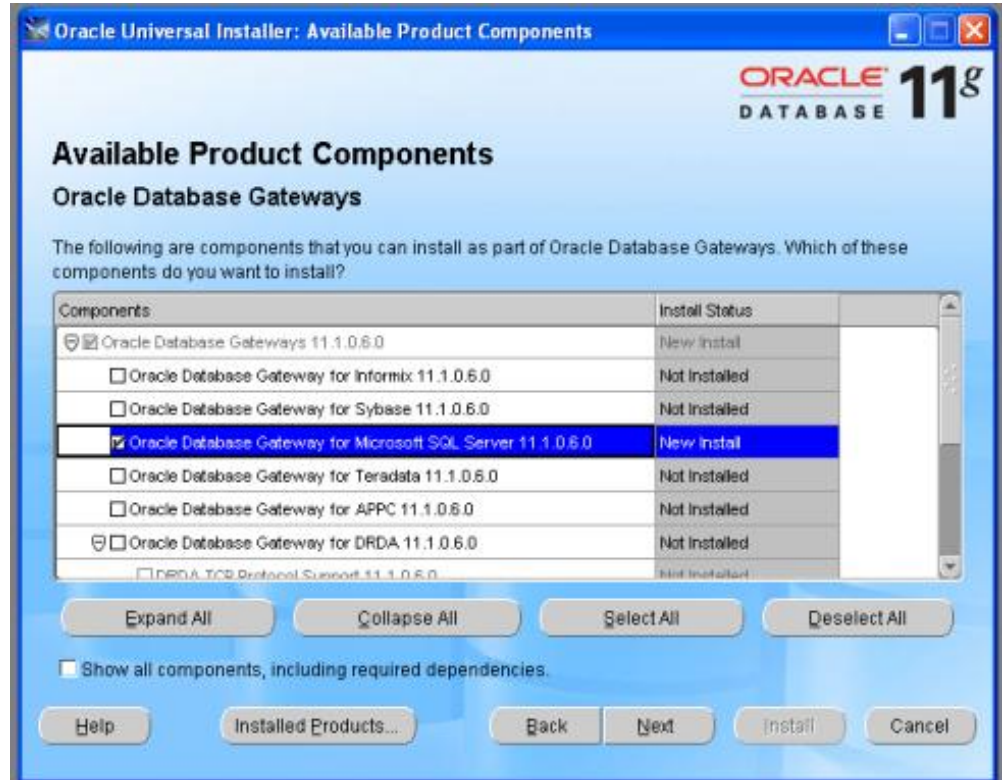
- Select the Oracle Database Gateways 11.1.0.6.0.



- Select the Oracle Home directory, for the database on which the gateway is to be installed.



- Select the Oracle Database gateway for Microsoft SQL Server 11.1.0.6.0.



- Enter the SQL server connection details as required.



- Click Next.
- Click Install and the gateway will start installation.



Tip: This will take few minutes.



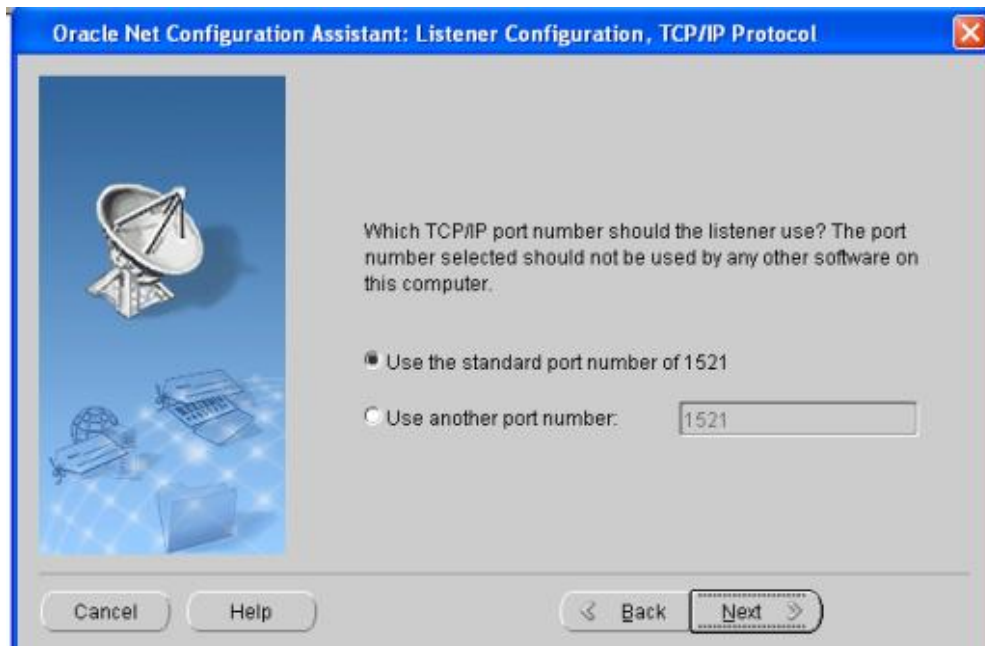
- Once the installation is complete the Oracle net configuration Assistant pops up for setting up the Listener for the gateway.

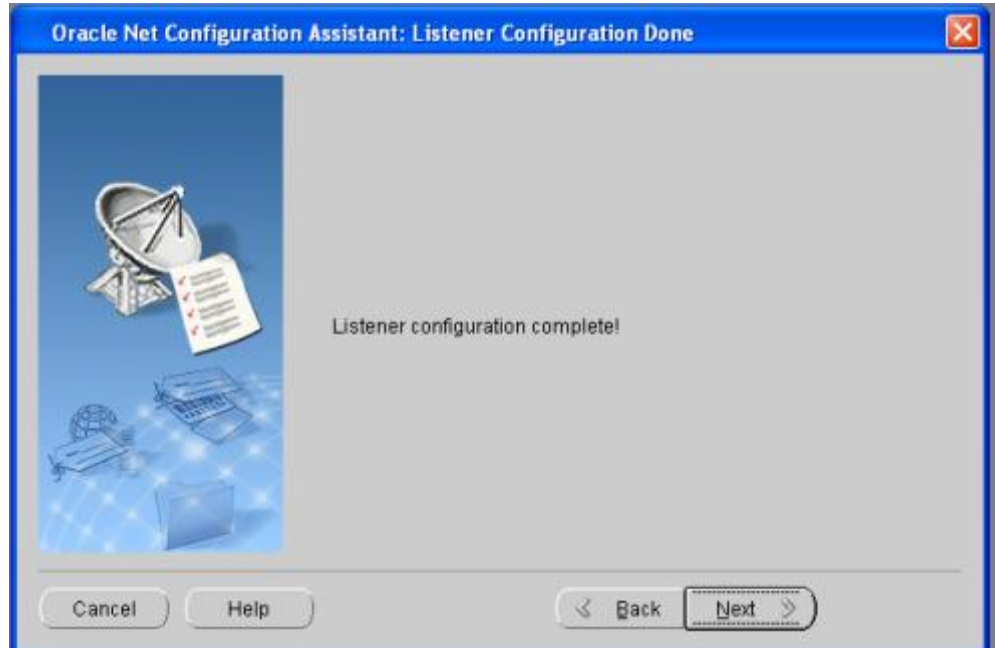




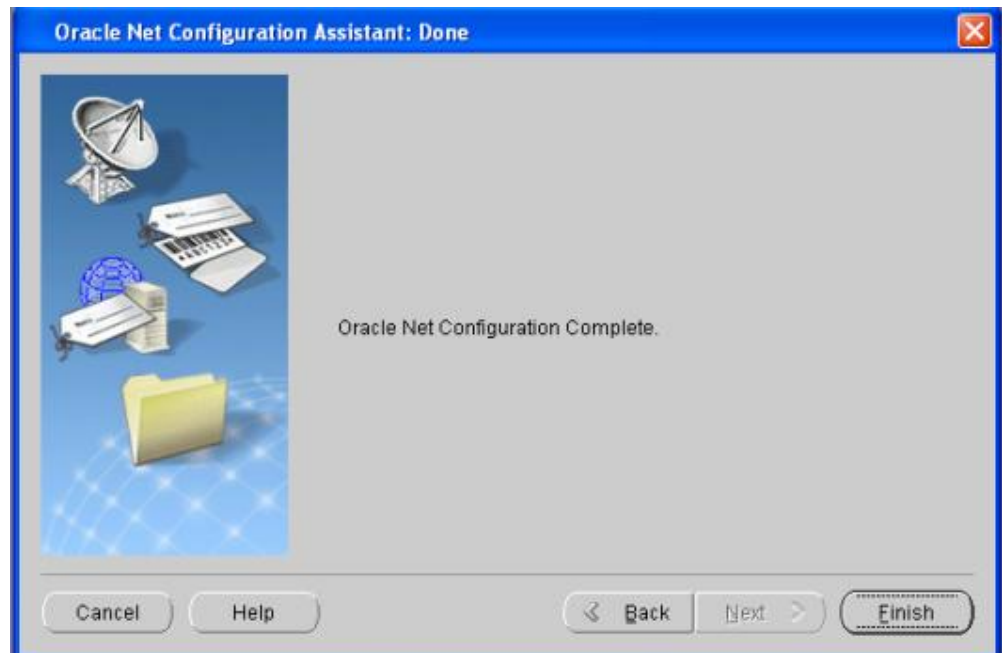
- Assign the Listener an appropriate name.





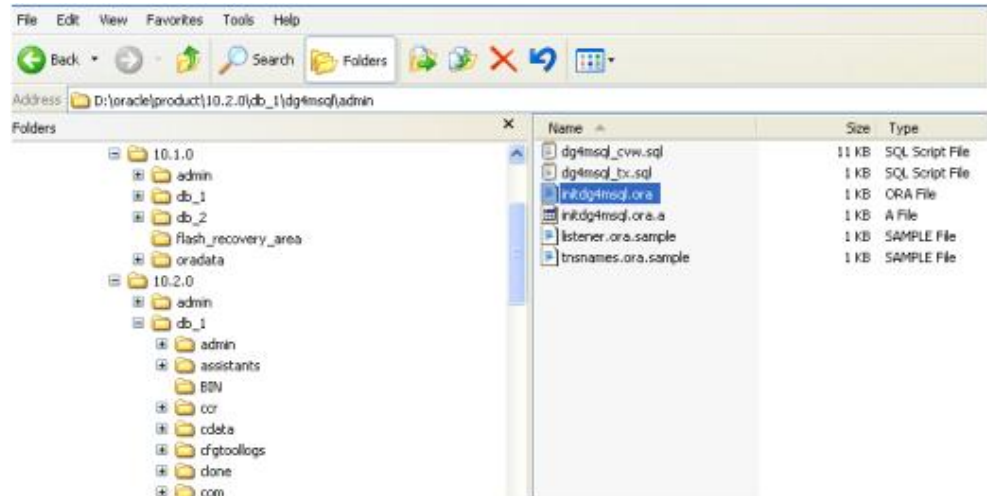


- Once the listener configuration is complete, keep clicking the "next" till the configuration is successfully complete.

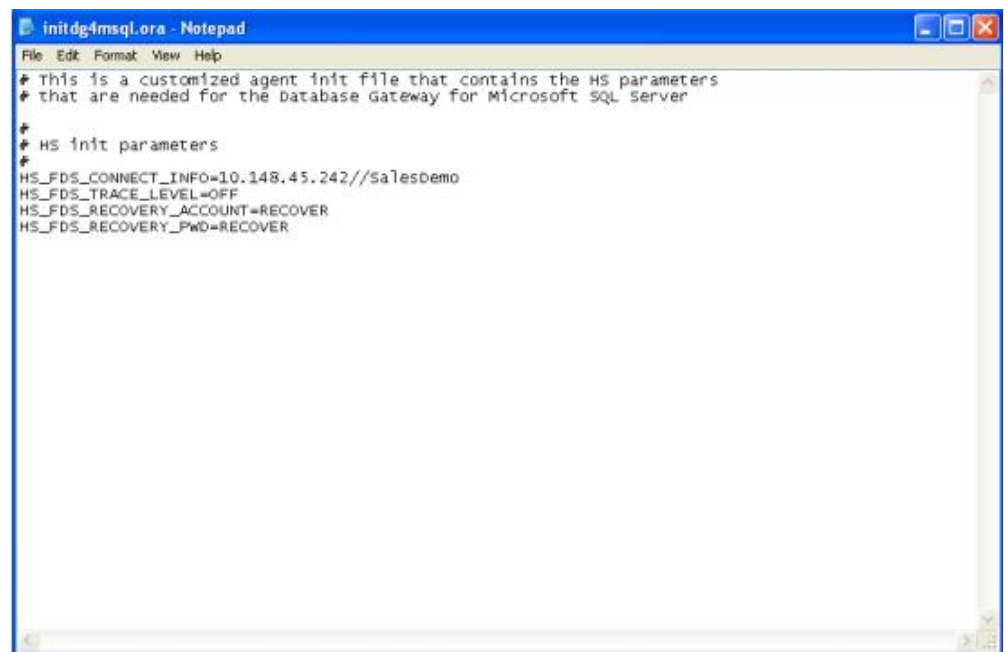




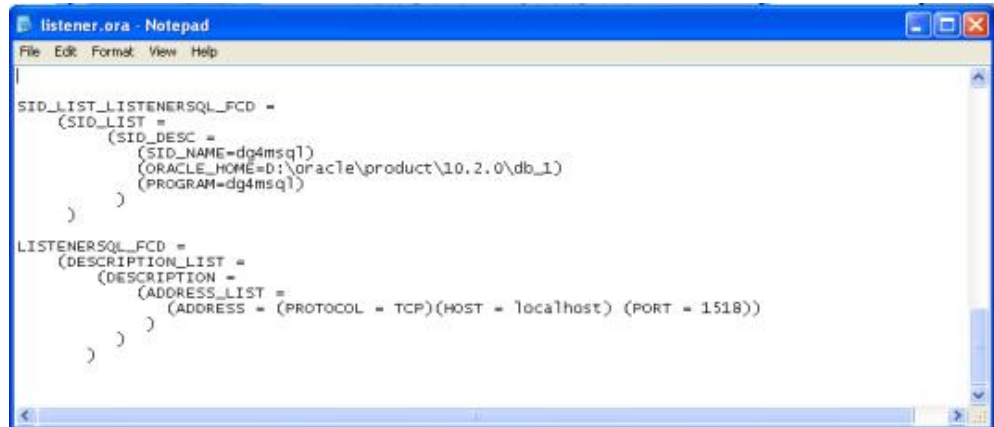
- Once the gateway has been successfully installed, you can find the folder for the database gateway in the Oracle home directory.



The initdg4msql.ora file is also present in dg4msql\admin. The initdg4msql.ora file contains the connection details that you defined earlier:

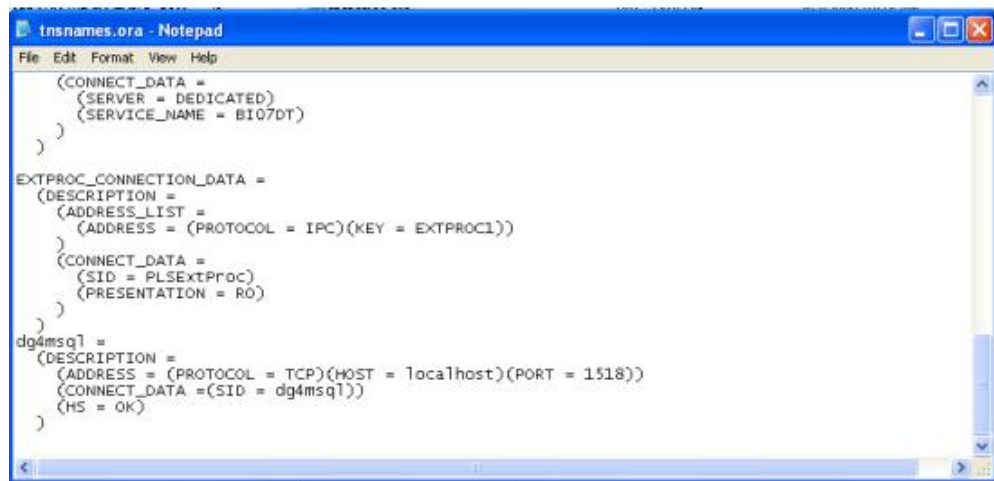


Modify the Oracle Home\NETWORK\ADMIN listener.ora as shown below for the Listener added. Restart the Listener.

A screenshot of a Notepad window titled 'listener.ora - Notepad'. The window shows the configuration for the listener. The content is as follows:

```
SID_LIST_LISTENERSQL_FCD =  
  (SID_LIST =  
    (SID_DESC =  
      (SID_NAME=dg4msql)  
      (ORACLE_HOME=D:\oracle\product\10.2.0\db_1)  
      (PROGRAM=dg4msql)  
    )  
  )  
  
LISTENERSQL_FCD =  
  (DESCRIPTION_LIST =  
    (DESCRIPTION =  
      (ADDRESS_LIST =  
        (ADDRESS = (PROTOCOL = TCP)(HOST = localhost) (PORT = 1518))  
      )  
    )  
  )
```

- Modify the tnsnames.ora in Oracle Home\NETWORK\ADMIN to add the dg4msql details.

A screenshot of a Notepad window titled 'tnsnames.ora - Notepad'. The window shows the configuration for the database link. The content is as follows:

```
(CONNECT_DATA =  
  (SERVER = DEDICATED)  
  (SERVICE_NAME = BI07DT)  
)  
  
EXTPROC_CONNECTION_DATA =  
  (DESCRIPTION =  
    (ADDRESS_LIST =  
      (ADDRESS = (PROTOCOL = IPC)(KEY = EXTPROC1))  
    )  
    (CONNECT_DATA =  
      (SID = PLSEXPProc)  
      (PRESENTATION = RO)  
    )  
  )  
  
dg4msql =  
  (DESCRIPTION =  
    (ADDRESS = (PROTOCOL = TCP)(HOST = localhost)(PORT = 1518))  
    (CONNECT_DATA = (SID = dg4msql))  
    (HS = OK)  
  )
```

- Create database link in the oracle database:
Create database link <Database link name>
Connect to <"Login"> identified by <"Password">
Using 'dg4msql'
- Database Link name to be used (for running the scripts): GRCM771_APPS_DBLINK
- Connect to the SQL database using this database link to load the data.

Using SQL Developer to view the data in SQL server directly from Oracle will result in errors if the source table contains nvarchar type columns. You can validate the link by using SQL plus to connect using the database link to the SQL server. Once the data is loaded in the tables, you can view it using SQL developer.

Creating the Target Physical Model

Open and compile each of the following package files in the Oracle Client:

Note: Since some of the scripts contain Unicode characters, they might show errors when opened in oracle clients like SQL developer. To avoid this, open the scripts in textpad or notepad, then copy and paste the scripts into the Oracle client to compile them.

- Constants_Create_pkg.sql
- Dims_Create_pkg.sql
- Facts_Create_pkg.sql
- Stage_Create_Pkg.sql

Run the following script. This step will create all the physical tables in the target schema. The caller has the option of forcing the table to be dropped and created based on value set for v_ForceCreate variable.

It also creates the source stage tables.

Execute_Create.sql

Note: If you are upgrading from an older version of GRCI, please force create the GRCD_USERS table by setting the value of v_ForceCreate to "1" while running the Execute_Create.sql (CreateUsers procedure) Else if the tables already exists (with the structure of Rel 2), DONOT set v_ForceCreate to "1" i.e. force create the table again as it will lose the existing data. Recreating the GRCD_TIME_D and GRCD_TIME_TL is not required if these tables are also present in the database. If recreating please make sure that the same values of the start and end year are given.

Run the following script to create the indexes and views in the target schema.

Execute_Index_View.sql

Loading Target Tables

Open and compile each of the following package files in the Oracle Client.

- Constants_Load_pkg.sql
- Dims_Load_pkg.sql

- Facts_Load_pkg.sql

Note: If the GRC Manager web application is not installed on your machine, you will need to set the v_GRCAApplication variable (found in Constants_Load_pkg) to reference the correct machine/ip address that is hosting the GRC Manager application.

Note: If the OBIEE installation is not installed on this machine you will need to set the v_OBIEEApplication variable (found in Constants_Load_pkg) to reference the correct machine/ip address that is hosting the OBIEE application.

Run the following script. This step loads all of the tables in target schema.

Note: While running the scripts, to insert data into the stage area, the variable v_SourceName is to be given as per the source type (SQLSERCER/ORACLE). If it is an SQL Sever source it should be given as "SQLSERVER" and for Oracle it should be given as "ORACLE".

Execute_Load.sql

You can repeat this step for several consecutive loads.

Installing OBIEE Reports

Introduction The GRI_20_OBIEE.zip contains two zip files:

- GRCDiagnostic.zip
- GRCDWebcat.zip

These files contain the repository and web-catalog, and are used in the steps below to install the repository and reports-dashboards respectively.

1. After you successfully install OBIEE (OBIEE version 10.1.3.3.3), extract the delivered zip file GRCDiagnostic.zip. Place the GRCDiagnostic.rpd file in the C:\OracleBI\server\Repository folder.
2. In the C:\OracleBI\server\Config folder, edit the NQSConfig.INI file. Enter the name of the RPD file after "Star =" in the [REPOSITORY] section.
3. Place the GRCDWebcat.zip file in the C:\OracleBIData\web\catalog folder and unzip the file. The GRCDWebcat folder now appears in the Catalog folder.
4. In the C:\OracleBIData\web\config folder, edit the instanceconfig.xml file. Enter

the path of the GRCDWebcat folder in between the <CatalogPath> tags.

5. Create the TNS entry to point to your GRCI schema in Oracle home directory.
6. Open the GRCDiagnostic.rpd in the Oracle BI Administration Tool and go to the Variable Manager under the Manage > Variables menu.
7. Update the GRI_DSN variable with the name of the TNS entry name.
8. Update the GRI_USER_ID with the database user ID.
9. Open the properties window for 'GRC Diagnostics > GRCI Connection Pool' in the Physical layer and provide the password for GRCI schema.
10. Save the changes in the Oracle BI Administration Tool.
11. Restart the Oracle BI Services.
12. Log into the OBIEE using this URL: <http://<localhost>:<TCPport>/analytics>, where <localhost> is the name of the machine or the IP address where OBIEE is installed, and <TCPport> is the Web Site TCP Port number.
13. The OBIEE login page loads.
14. The installation is now complete.

Multi-Language Setup for OBIEE

The source language files required to support multiple languages in OBIEE are located in the GRI_20_GRCM_OBIEE_LANG.zip file.

They are present in the captions.zip file.

Currently there are 11 supported languages:

1. Danish (da)
2. German (de)
3. Spanish (es)
4. French (fr)
5. French Canadian (fr-ca)
6. Italian (it)
7. Japanese (ja)

8. Korean (ko)
9. Portuguese Brazilian (pt-br)
10. Chinese (zh)
11. Chinese Traditional (zh_tw)

Follow the procedure mentioned below to include the language files in the OBIEE server. This procedure must be followed after installing OBIEE and before starting the OBIEE server.

Note: If the "res" folder is not already present then create this folder in the "web" folder.

- 1. Unzip the captions.zip file present in the GRCI_20_GRCM_OBIEE.zip file into "OracleBIData\web\". Check if the folder structure matches as shown below in Figure 1.

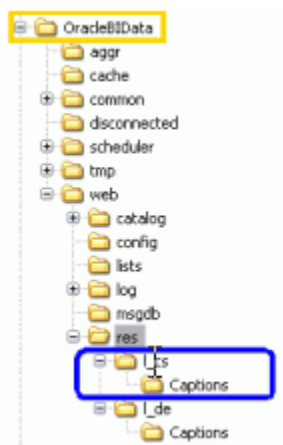


Figure 1

- 2. Copy the "GRCDiagnostic.xls" file present in the GRCDiagnostic.zip to the OBIEE Server Repository folder. The location is "OracleBI\server\Repository\".
- 3. Create the System DSN named 'LANGUAGE_POOL' and configure it to point to the "GRCDiagnostic.xls" that was copied to the location mentioned in Step 1.
- a) Use the Administrative Tools => Data Sources (ODBC) to create the DSN. Select the Microsoft Text Driver as shown below in **Figure 2**.

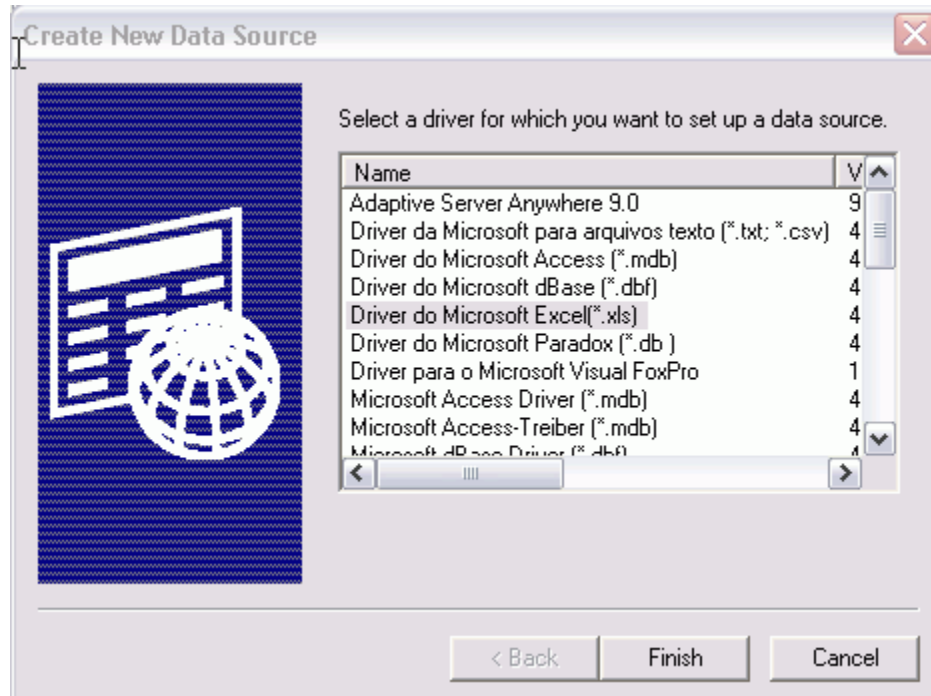


Figure 2

- b) Provide the Data Source Name as LANGUAGE_POOL. Use the "Select Workbook" and select the "GRCDiagnostic.xls" in the Repository folder that we copied in step 2.

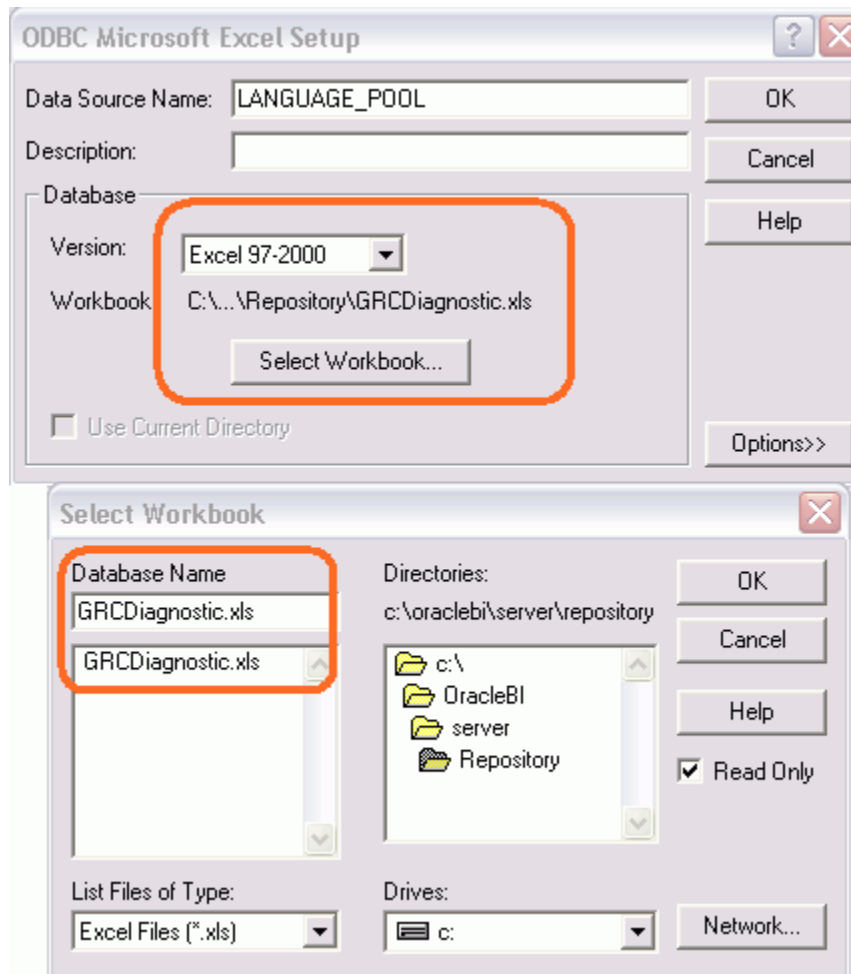


Figure 3

- 4. To confirm your configurations, Open the GRCDiagnostic.rpd using OBIEE => Administration. Verify that the DSN specified in the Connection Pool for the database "LANGUAGE_POOL" is pointing to the "LANGUAGE_POOL" DSN that we created in Step 2 as shown in Figure 3.

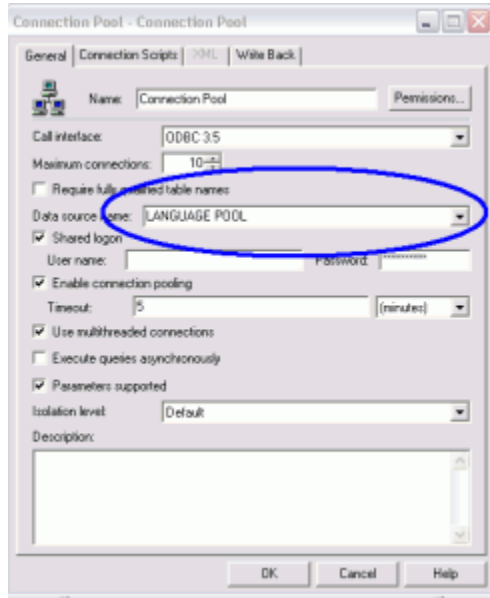


Figure 4

- 5. Once the connection is established you can verify the data by right clicking on the "GRCDiagnostic.xls" folder in the physical layer of the rpd and select "View Data" as shown in **Figure 5**.

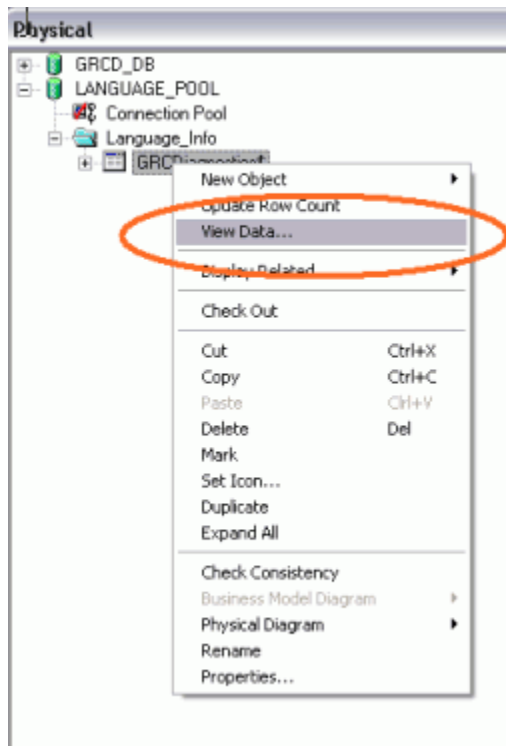


Figure 5

View Data from Table "LANGUAGE_POOL"."Language_L..."

16060 rows ☐ Distinct Query

Show 100 rows starting from 0 Close

	ACTUAL	LANGUAGE	SESSION
0	Presentation Catalog Assess: en		CN_Assessme
1	Presentation Table Assess: en		CN_Assessme
2	Presentation Column Assess: en		CN_Assessme
3	Presentation Column Assess: en		CN_Assessme
4	Presentation Column Assess: en		CN_Assessme
5	Presentation Column Assess: en		CN_Assessme
6	Presentation Column Assess: en		CN_Assessme
7	Presentation Column Assess: en		CN_Assessme
8	Presentation Column Assess: en		CN_Assessme

Figure 6

Note: If the rows are visible as shown in **Figure 6**, then the connection has been setup correctly.

Now after the connection is established using the connection pool, use the Language drop down list to select the required language before logging in to OBIEE Presentation Service as shown below in **Figure 7**. This will display the application in the selected language.



Figure 7

Installing BI Publisher Reports

BI Publisher Installation

Install Oracle BI Publisher (10.1.3.3.3). Use the Basic installation option that provides OC4J, Sun JDK, with BI Publisher. Refer the 'Oracle Business Intelligence Publisher Installation Guide' for environment requirements and other details.

Data Source Configuration

Connect to BI Publisher server. Go to 'Admin > JDBC' tab. Click 'Add Data Source' link. The following window appears.

The screenshot shows the 'Add Data Source' window in the Oracle BI Publisher Enterprise application. The window is titled 'Oracle BI Publisher - Microsoft Internet Explorer'. The address bar shows the URL: <http://dhcp-amer-csvpn-gw1-141-144-65-66.vpn.oracle.com:9704/xmlpserver/>. The main content area has a blue header with the Oracle logo and 'BI Publisher Enterprise'. Below the header, there are tabs for 'Reports', 'Schedules', and 'Admin'. The 'Admin' tab is selected, and the breadcrumb path is 'Admin > JDBC > Add Data Source'. The 'Add Data Source' form has a 'General' tab selected. It contains the following fields and controls:

- * Data Source Name: Text input field.
- * Connection String: Text input field with a dropdown arrow on the right.
- * Username: Text input field.
- Password: Text input field.
- * Database Driver Class: Text input field with a hint '(Example: oracle.jdbc.driver.OracleDriver)' below it.
- ☐ Use Proxy Authentication: Checkbox.
- Test Connection: Button.
- Cancel: Button.
- Apply: Button.

Figure 8

Enter the following information as given below. Use the appropriate connection information for the content in the <> brackets.

Data Source Name: **GRCD**

Connection String

Reporting DB Platform

Oracle

Connection String

jdbc:oracle:thin:@<host name>:<port num>:<service name>

Driver Name

Reporting DB Platform

Oracle

Driver Name

oracle.jdbc.driver.OracleDriver

Click the 'Test Connection' button to check the successful connection establishment. Then click 'Apply' button to save the data source connection information. Refer to **Figure 9**.

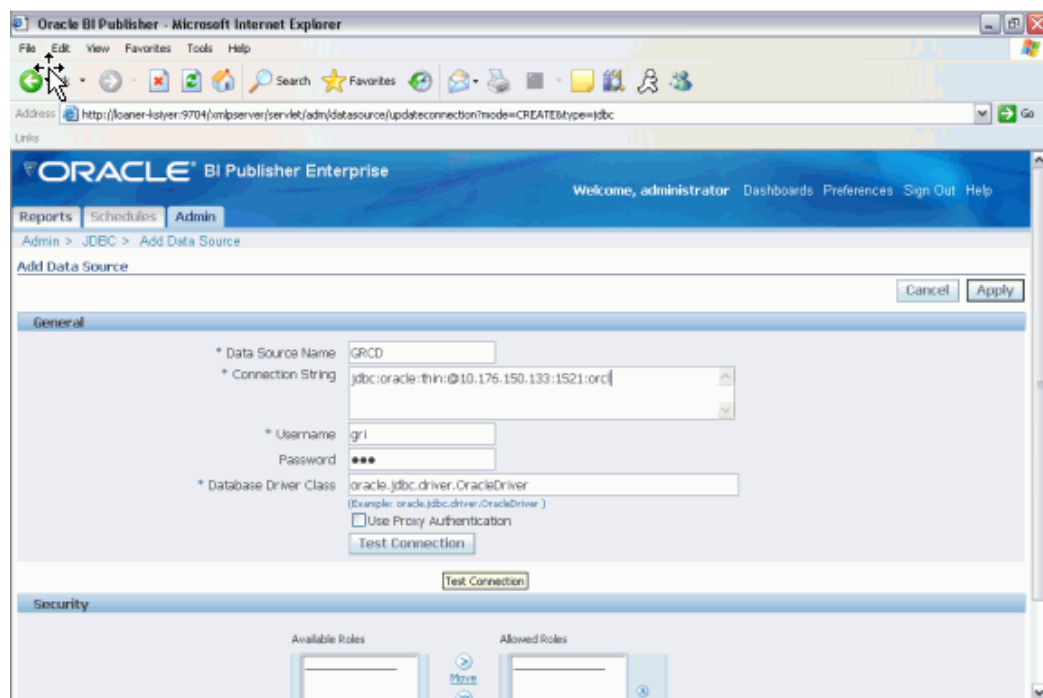


Figure 9

Report Configuration

- Stop the BIP Service.
- Extract the delivered zip file GRCI_20_GRCM_BIP.zip.

- 3. Extract the BIP_Reports_base.zip and BIP_Reports_lang.zip into the same "Reports" folder. Copy the folders under "Reports" folder to the report metadata to the directory <Oracle BI Publisher Home>\xmlp\XMLP\Reports\. Refer to **Figure 10**

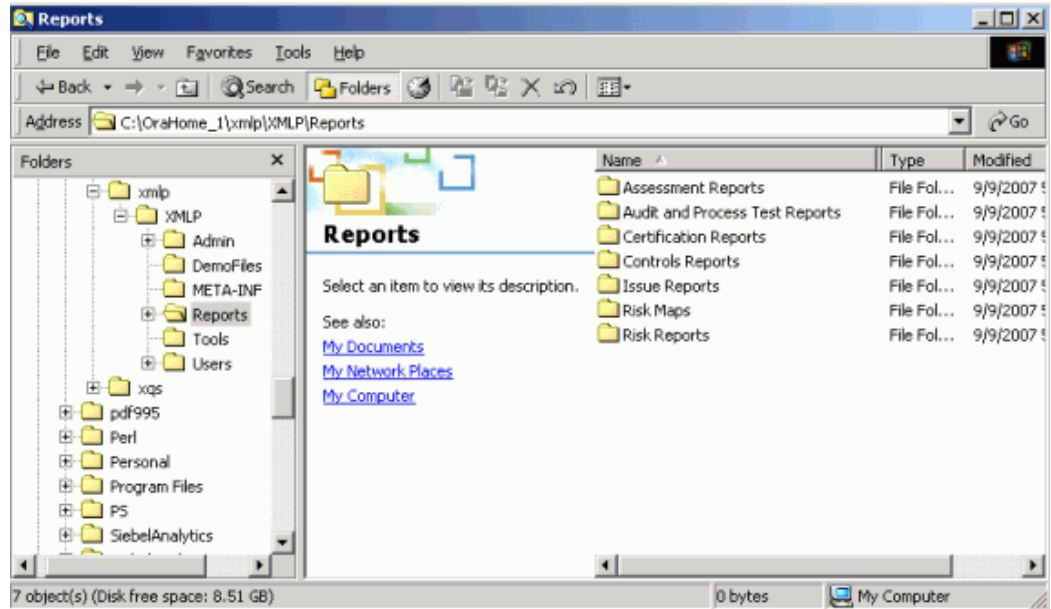


Figure 10

- Restart the service.
- Connect to BI Publisher Server. Go to 'Reports' tab and check if the following report folders are available as shown in **Figure 11**:
- Assessment Reports
- Audit & Process Test Reports
- Certification Reports
- Control Reports
- Issue Reports
- Risk Maps
- Risk Reports

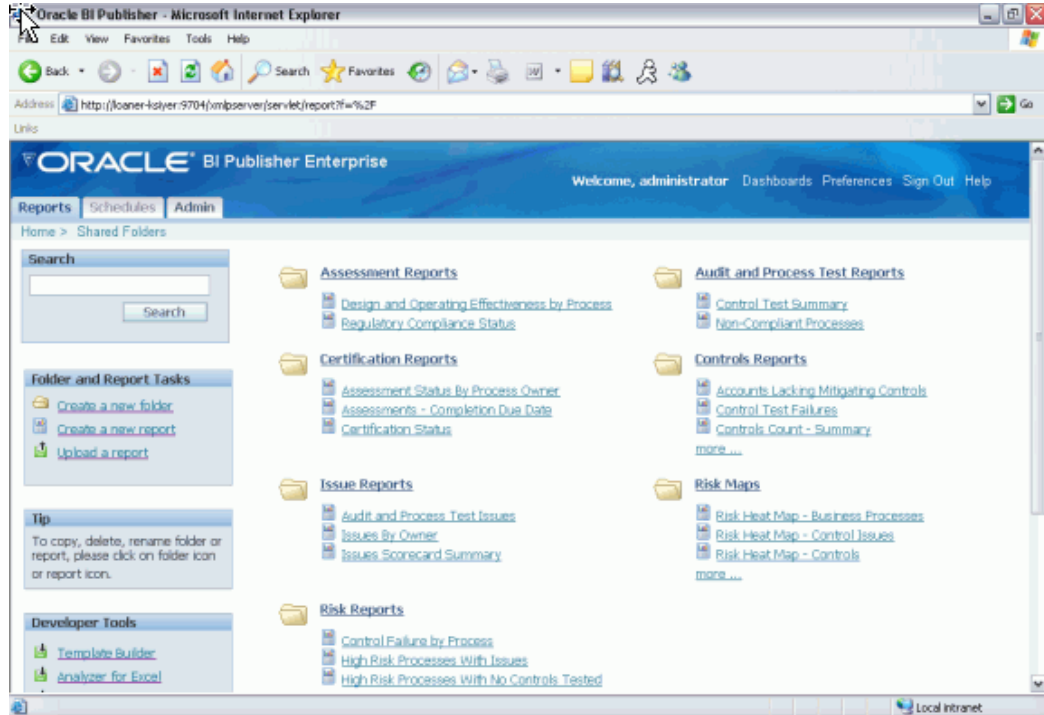


Figure 11

Security Integration with GRCM (Optional)

This section provides details on integrating the security component of two applications: GRCM and GRCI to satisfy the following requirements:

1. All GRCM users available in GRCI , without the need to recreate them.
2. Ability to launch a GRCI dashboard from GRCM application without having to sign-on.
3. Ability to launch a GRCI answer from GRCM application without having to sign-on.

The ideal solution to satisfy the above requirements would be to integrate GRCM and GRCI using the combination of LDAP (Light weight directory access protocol) and SSO (Single sign-on) servers. This solution provides a quick fix to integrate the security component of the two applications using the 'External Table Authentication' feature of OBIEE (Oracle Business Intelligence Enterprise Edition) and it can be used in implementation sites, which do not have LDAP and SSO.

1. Create and load table to store GRCI users.

The procedure to load the table GRCD_Users is executed as part of the GRCD data load and it reads data from the GRCM tables Users and UserSecurityAttributes. After the

load is complete, all the GRCM users and roles are available in the table GRCD_Users, which then acts as an identity store for GRCI. As rows (which represent users and roles) are created in the table a proxy password of 'Password' is used.

- All users are assigned a default password of 'Password', which is stored in clear-text form in the table GRCD_Users. During implementation, OBIEE administrator can change the password as desired but it can be stored only in clear-text form and all users must have the same password.
- Since the table GRCD_Users also stores user information related to AACG users, it contains users from both GRCM and AACG, identified by the SRC_SYS_ID column.

The procedures CreateUsers and LoadUsers load data into table GRCD_USERS if GRCM and GRCI are implemented in Oracle environment.

2. Modify the rpd (The GRCI repository data file) file to create Initialization block and session variables.

This section begins with modifications to the configuration file and proceeds to create the initialization block script and session variables in the repository (rpd) file. OBIEE uses this script to set the session variables when user launches the GRCI answer/dashboard from GRCM.

1. Shutdown Oracle BI Server and Oracle BI Presentation Server services.
2. Launch Oracle BI Administration tool. Open the rpd file (indicated in NQSConfig.ini ->[Repository] section -> Star entry) in offline mode.
3. From the Manage menu, click on Variables to launch the Variable Manager.
4. From the menu click on Action, Select New and choose Session->Initialization Block to create an initialization block. Name the block as GRCD Security.
5. In the Data Source section, click on Edit Data Source. From the Data Source Type drop-down box choose Database. In the 'Default Initialization String' window type the following SQL:

```
SELECT USERNAME, GROUPNAME, DISPLAYNAME, LOGLEVEL
FROM GRCD_Users
WHERE USERNAME=':USER'
AND PASSWORD=':PASSWORD'
```
6. The Connection Pool should display 'not assigned'. Click on Browse to launch the Select Connection Pool window. Click on the appropriate Connection Pool and click Select, then click OK.
7. In the Variable Target section, click on Edit Data Target. Click New to launch the Session Variable window. In the name box enter USER. Click OK. Accept the

'special purpose' prompt by clicking on Yes.

8. Similarly add variables GROUP, DISPLAYNAME, LOGLEVEL, assigning the GRCD Security as initialization block to all of them. Add a default initialization value of 2 for LOGLEVEL variable.
9. Enable the 'Required for Authentication' check box.
10. Save the initialization block GRCD Security.

3. Create repository groups corresponding to GRCM roles and secure presentation layer catalogues.

The GRCM roles are loaded by the sql script into the GRCD_Users table (GROUPNAME column). Use these roles to create repository groups in the rpd files and associate only the presentation catalogues that need to be accessed by these roles. So, when you connect to the dashboard, only the presentation catalogues that are attached to the user's role are available as 'Subject Areas' for creating answers.

Note: The GRCM role SOAExternalAudit and the presentation catalog GRC Diagnostics Detail are used as examples in the next section.

1. Open the GRCM rpd in OBIEE Administration tool and logon with admin privileges.
2. Click on Manage->Security from the menu.
3. On the Security Manager window, select Groups in the left pane and click on Action->New->Group.
4. From the GROUPNAME column of the GRCD_Users table, select a group (for example, SOAExternalAudit) and enter that as name of the group. Click OK. The group is created in the repository.
5. To secure a catalog in presentation layer by the group, right click on the catalog (GRC Diagnostics Detail), click Properties and click on Permissions tab.
6. In the Permissions window, make sure that 'Show all users/groups' check box is selected. Locate the group that was added in Step 3 and below the 'Read' column click on the check box until it becomes a tick mark, granting access to the (SOAExternalAudit) group.
7. Right click on another catalog (GRC Diagnostics Overview), click Properties and click Permissions tab.
8. In the Permissions window, make sure that 'Show all users/groups' check box is selected. Locate the group that was added in Step 3 and below the 'Read' column

click on the check box until it becomes a red x mark, preventing access to the (SOAExternalAudit) group.

9. Upon completion of steps 6 and 8, the group SOAExternalAudit has access to GRC Diagnostics Detail subject area but not to GRC Diagnostics Overview subject area. (The names of groups and presentation catalogues/subject areas are used as examples here).
10. Click OK. Save the rpd.

4. Create presentation catalog group and secure dashboards, folders and answers

The GRM roles are loaded by the sql script into the GRCD_Users table (GROUPNAME column). Use these roles to create presentation catalog groups and associate dashboards to each group. So, when the user launches a GRCI report/dashboard from GRM, only the dashboards associated with the user's role will be displayed. No other dashboards can be accessed by the user.

1. Connect to OBIEE Presentation server and log on as Administrator.
2. Click on Settings->Administration and select 'Manage Presentation Catalog Groups and Users' and click on 'Create new catalog group'.
3. Enter the group name from GRCD_Users.GROUPNAME column, in the Group Name, Dashboard Name and Dashboard Builder columns of the Create Catalog Group screen. (For instance, use SOAExternalAudit).
4. OBIEE creates a folder under 'Shared Folders' and an empty dashboard with the name specified in Step 3.
5. Repeat Step 3 until dashboards and presentation service groups are created for all GRM roles.
6. Click Finished and return to Oracle BI Presentation Services Administration screen. Click on 'Manage Interactive Dashboards' to verify the list of all the dashboards. Click Finished. Similarly click on 'Manage Presentation Catalog' to verify that the new presentation service groups appear as folders below Shared Folders. Click Finished. Click Close Window.
7. In the 'Answers' screen create desired reports (or move the existing reports) and store them below the folders created in Step 3.
8. Edit the dashboards created in Step 5 and add desired reports created in Step 6 to the dashboard sections.
9. To prevent/grant access to other dashboards, click on Settings->Administration and select 'Manage Interactive Dashboards'. The Manage Dashboards screen launches with a list of dashboards. Choose the dashboard that needs to be secured from the

role (SOAExternalAudit). Click on the Permissions icon in that dashboard and remove the public role 'Authenticated Users' from the list of users and groups that have explicit access to this item. Repeat this step for all dashboards that need to be secured from the catalog group (SOAExternalAudit). Similarly to grant access to a dashboard (for the GRCM role), choose the dashboard, click on Permissions icon in that dashboard and add the presentation service group to the list of users and groups that have explicit access to this item. At the end of this particular step the list of dashboards that can/cannot be accessed by the presentation service group is fixed.

10. To secure Folders and Answers, click on Settings->Administration and select 'Manage Presentation catalog'. The Manage Catalog screen launches with folders. Switch to Shared Folders. To secure a folder, click on the Permissions icon of the folder. Remove 'Everyone' from the list of users and groups that have explicit access to this item. Add only the presentation service group that should have access to the list of users and groups that have explicit access to this item. Click Finished when necessary folders have been secured. Similarly to secure a particular answer, click on the folder name that contains the answer. To secure an answer, click on Permissions icon of the answer. Remove 'Everyone' from the list of users and groups that have explicit access to this item. Add only the presentation service group that should have access to the list of users and groups that have explicit access to this item. Click Finished when necessary answers have been secured.
11. Logoff and restart OBIEE services.
12. Log on as a GRCM user (associated with SOAExternalAudit role for instance) into GRCD. Only the dashboards that are accessible to the presentation services group associated with the GRCM user should be displayed and the user shouldn't have access to any other dashboard. Click on Answers. Only the folders and answers that are accessible to the presentation services group associated with the GRCM user should be displayed and the user shouldn't have access to any other folder or answer.

5. Modify menu.aspx file to launch GRCD from GRCM menu

This section describes the modifications to be made to menu.aspx, which can be located in the \Inetpub\wwwroot\OracleGRCManager\Nav directory. These modifications enable the OBIEE based GRCI dashboard to be launched within the GRCM (FCD) application.

Add the following functions to the JavaScript section of the menu.aspx file:

```
function OBIEE_redirect()
{
parent.frames['main'].location.href="<%=mConfig.Constant("ADVREPORTINGBASEURL")%
>/saw.dll?Dashboard&NQDV1=24523452345235&NQDV2=24523452345235&NQUser=<%=mState.LoginId%
>&NQPassword=Password";
self.status = '';
}
function click()
{
if (event.button == 2){
return false;
}
}
}
```

and just before the end of the JavaScript block add these two lines of code:

```
document.onmousedown = click;
document.oncontextmenu = new Function("return false");
```

Locate the section:

```
<tr id="mnuAdvReporting" runat="server">
<td class="t-vspacer"></td>
<td class="VNLevel2">&nbsp;
<a href="<%=mConfig.Constant("ADVREPORTINGBASEURL")%>/saw.dll?Dashboard
....
....
..
</td>
<td class="t-vspacer"></td>
</tr>
```

and modify the section as:

```
<tr id="mnuAdvReporting" runat="server">
<td class="t-vspacer"></td>
<td class="VNLevel2">&nbsp;
<a href="javascript:OBIEE_redirect();" />
....
....
...
</td>
<td class="t-vspacer"></td>
</tr>
```

As seen above, the function of OBIEE_redirect() contains a proxy password of 'Password', the same as referred to in 'Create and load table to store GRCD users' section of this document. If you change the password in GRCD_Users table, it should also be modified in the function OBIEE_redirect().

Save the menu.aspx file.

6. Modify the GRCI views to include a JavaScript call to GRCM pages so that drill from GRCI to GRCM happens seamlessly

The drill across from GRCI to GRCM (drill back to source) is available out of the box and this section helps by making that experience seamless.

Note: This section is only applicable in situations where the GRCI dashboard is launched from GRCM. If the GRCI dashboard will only be launched external to GRCM (for instance, by launching the GRCI dashboard URL directly) this modification to the procedures is NOT required.

GRCI dashboards like Certifications have links to GRCM which provide insight on the source data. For instance, the answer 'Assessments - Completion Due Date' which is available in the Certifications dashboard contains a column called Process Title which acts as a link to the process information in GRCM. When this column is clicked, the process page in GRCM is launched with details of the process, within the same frame (without the need to switch to another GRCM window), thus providing better user experience. When the browser's back button is clicked the context switches back to the GRCI dashboard. This section describes the steps involved in updating a URL column in a GRCI view with a JavaScript call, which provides this functionality.

Note: The steps below explain how to add the JavaScript call to the view GRCD_PROCESS_V only and it uses the document type SOA_BPC. Repeat the steps for the views GRCD_ASSESSMENT_V, GRCD_CONTROL_V, GRCD_ISSUE_V, GRCD_CONTROL_TEST_V and GRCD_RISK_V using the appropriate document type.

- Edit the view GRCD_PROCESS_V in query editor or open the file that contains the procedure in a query editor.
- If the environment is MSSQLServer, locate the column:

```
'<a href="'+b.URL+'/Nav/Redirect.aspx?doctype=SOA_BPC&id='+a.dDocName+'">' +a.Title+'</a>' URL,
```

and modify it to:

```
'<a href="javascript:window.top.location='''+b.URL+'/Nav/Redirect.aspx?doctype=SOA_BPC&id='+a.dDocName+''';">' +a.Title+'</a>' URL,
```

- If the environment is Oracle, locate the column:

```
'<a href="'+b.URL+'/Nav/Redirect.aspx?doctype=SOA_BPC&id='+a.dDocName+'">' +a.Title+'</a>' URL,
```

and modify it to:

```
'<a href="javascript:window.top.location='''||b.URL||'/Nav/Redirect.aspx?doctype=SOA_BPC&id='||a.dDocName||''';">' ||a.Title||'</a>' URL,
```

and remember to use SET DEFINE OFF to suppress the substitution variable, if you are using an editor like SQL*Plus.

1. Drop and recreate the view. Save the file.

7. Launch GRCM, switch to GRCI, drill back to GRCM

1. Login to GRCM application and locate the Dashboard link beneath Advanced Reporting menu item in the left pane and click on it to launch the GRCI dashboard in the right side frame.
2. The GRCI dashboard will launch with an empty home page, list of dashboards the role(s) associated with the user id can access (this was setup in previous sections) will be available in the top of the frame.
3. Click on a dashboard which has links to GRCM (for instance, Certifications) and click on a report column which appears as a hyperlink (for instance, the column Process Title in answer Assessments - Completion Due Date) to drill to details of that column in GRCM. Click the browser back button to switch back to GRCI.

Installing Oracle Fusion Governance, Risk and Compliance Intelligence for AACG 8.1.1 or Later

Overview

This chapter describes the steps necessary to install, configure and populate a GRCI 2.0 datastore sourced from AACG 8.1.1. The following section lists some scripts that need to be executed to create setup tables and load configuration data into the GRCI 2.0 datastore. The subsequent sections cover the installation of ODI projects, OBIEE reports, and an optional OAM based security integration.

Installing Oracle AACG Scripts

This section lists some scripts that need to be executed in order to create setup tables and load configuration data. The subsequent sections cover installation of ODI projects, OBIEE reports, and an optional OAM based security integration.

Steps to run the scripts for creation of the target and config tables. If you are installing GRC Intelligence Release 2.0 for GRC Manager and AACG, then AACG Scripts Installation should be completed first, followed by the GRC Manager Scripts Installation.

Execute the scripts provided in the following order:

Note: Since some of the scripts contain Unicode characters, they might show errors when opened in oracle clients like SQL developer. To avoid this, open the scripts in textpad or notepad, then copy and paste the scripts into Oracle client to compile them.

1. CreateTable.sql:

Drops and recreates the target tables, along with the sequences and index.

2. CreateConfigTables.sql:

Drops and recreates the configuration tables.

3. InsertData.sql:

Inserts (-1/-2) rows into dimension tables and also loads the seed data into the config tables (GRI_A_LOOKUP, GRI_A_LOOKUP_TL, GRI_A_DW_CONFIG_TBL and GRI_A_SRC_SYSTEM_INFO)

Note: When GRCI-AACG security integration implementation is required, update AACG host and port information in SOURCE_URL column of GRI_A_SRC_SYSTEM_INFO table. Use SET DEFINE OFF to suppress substitution value.

4. CreateTIME.sql:

Time create table package.

5. InsertTIME.sql:

This sql file creates the package ExecuteTIME.sql which loads the Time dimension GRCD_TIME and GRCD_TIME_TL.

6. ExecuteTIME.sql:

Execute the CreateTIME and InsertTime package to create and insert data into the GRCD_TIME and GRCD_TIME_TL tables.

7. CreateViews.sql:

Creates the views for the tables.

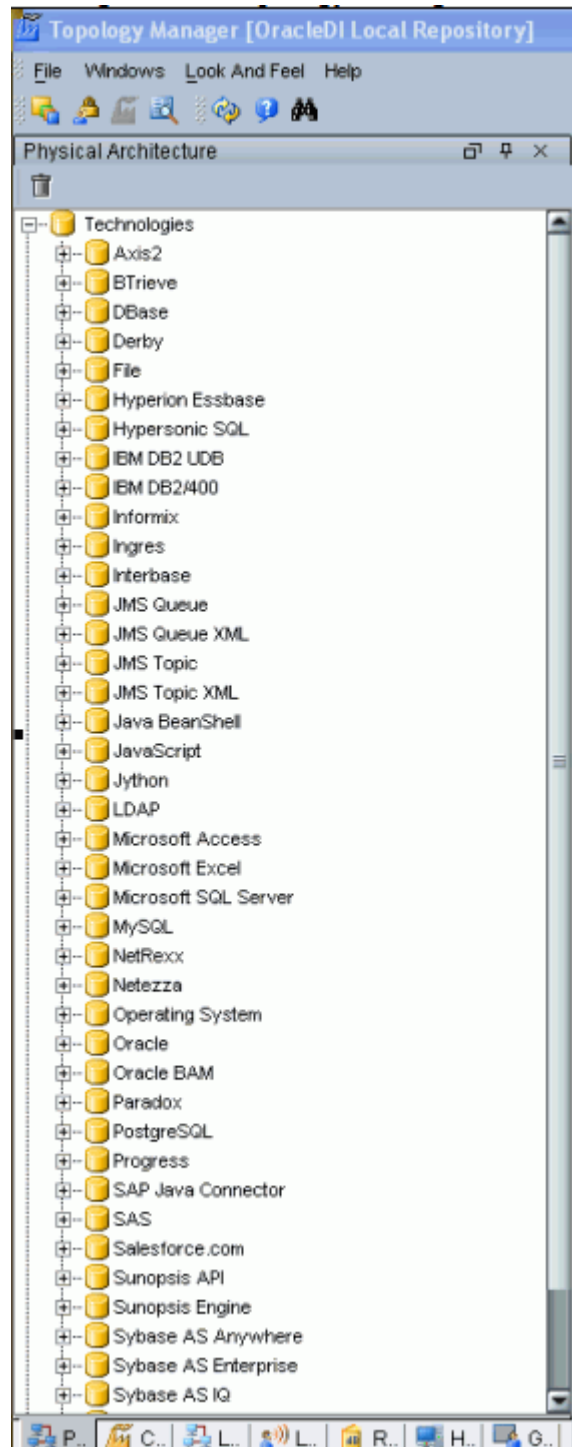
Installing ODI Code

The following steps describe the process used by ODI to extract the data from the staging tables populated by AACG data services, and then transforming and loading the data into GRCI datastore.

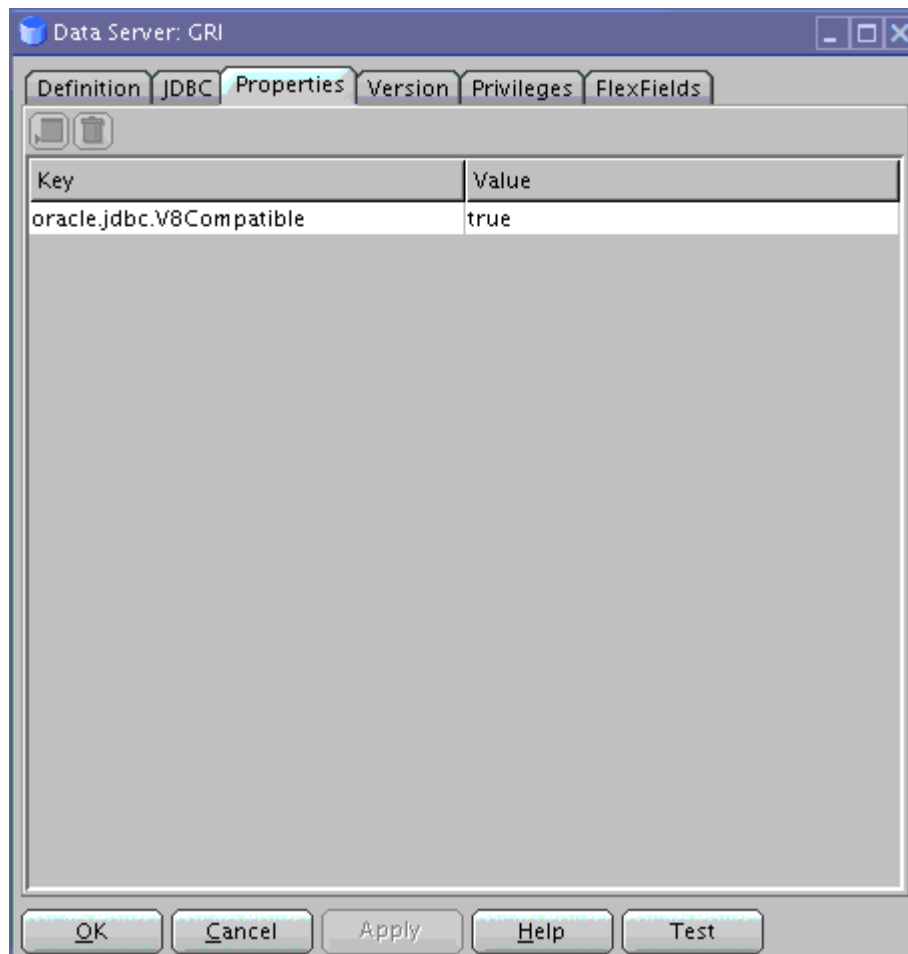
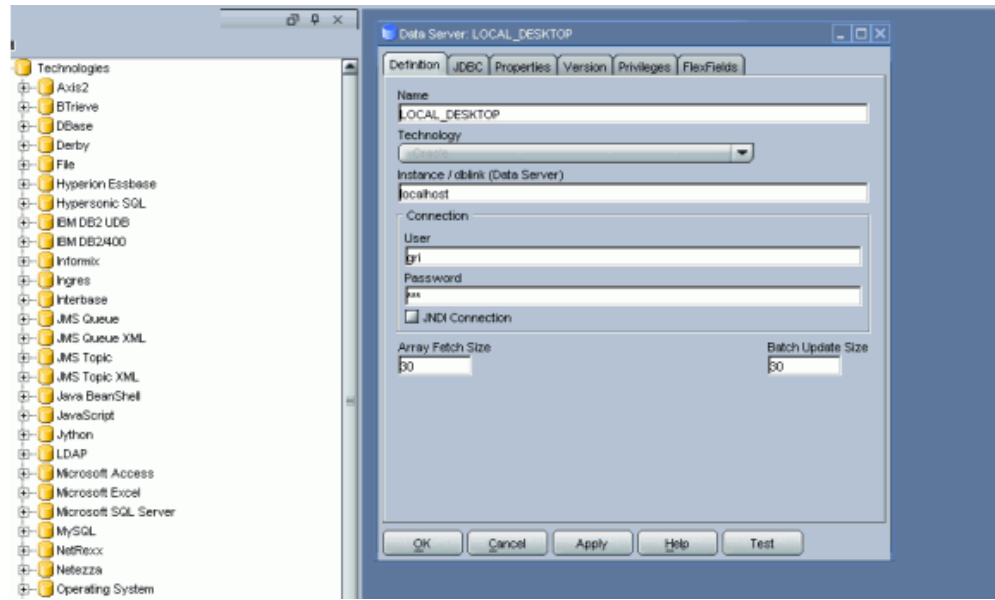
1. Create a Master Repository and Work Repository.

2. Create a Physical Connection:

Step 1: Login to the Topology Manager, switch to the Physical Architecture tab:



Step 2: Expand "Oracle" Physical Technologies and Insert a "New Data Server". Specify the details of the database where "GRI" schema is hosted. (In the JDBC tab provide the necessary information). Specify the login/privileges that will be used by the ETL processes.



Step 3: Once the data server information is saved, specify the "Insert Physical Schema" in the newly created data server, as shown (specify the "GRI" schema where GRI_% tables are stored as the physical schema in both Schema and Work Schema).

Physical Schema: LOCAL_DESKTOP.GRI

Definition Context Version Privileges FlexFields

Data Server: LOCAL_DESKTOP

Name
LOCAL_DESKTOP.GRI

Schema (Schema)
GRI

Schema (Work Schema)
GRI

☒ Default

Work Tables Prefix

Errors	Loading	Integration
E\$	C\$	\$

Journalizing elements prefixes

Datastores	Views	Triggers
J\$	JV\$	T\$

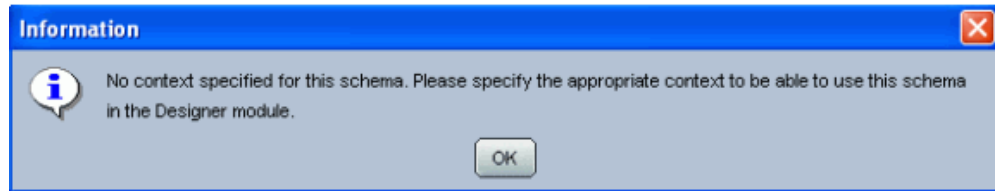
Naming Rules

Local Object Mask
%SCHEMA.%OBJECT

Remote Object Mask
%SCHEMA.%OBJECT@%DSERVER

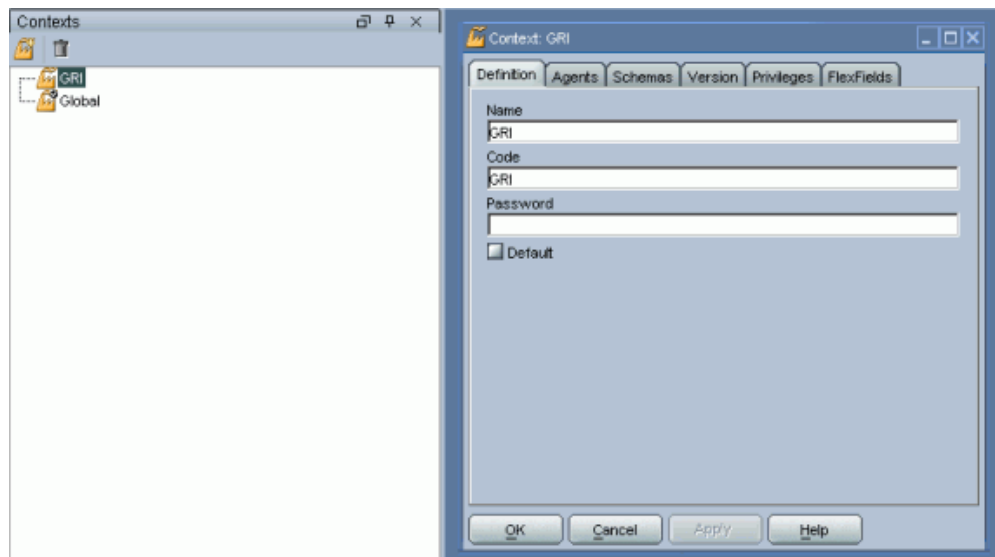
OK Cancel Apply Help

Step 4: Once you have saved the Physical Schema information, you will receive a Popup message asking for the "Context" for the physical schema, as shown.



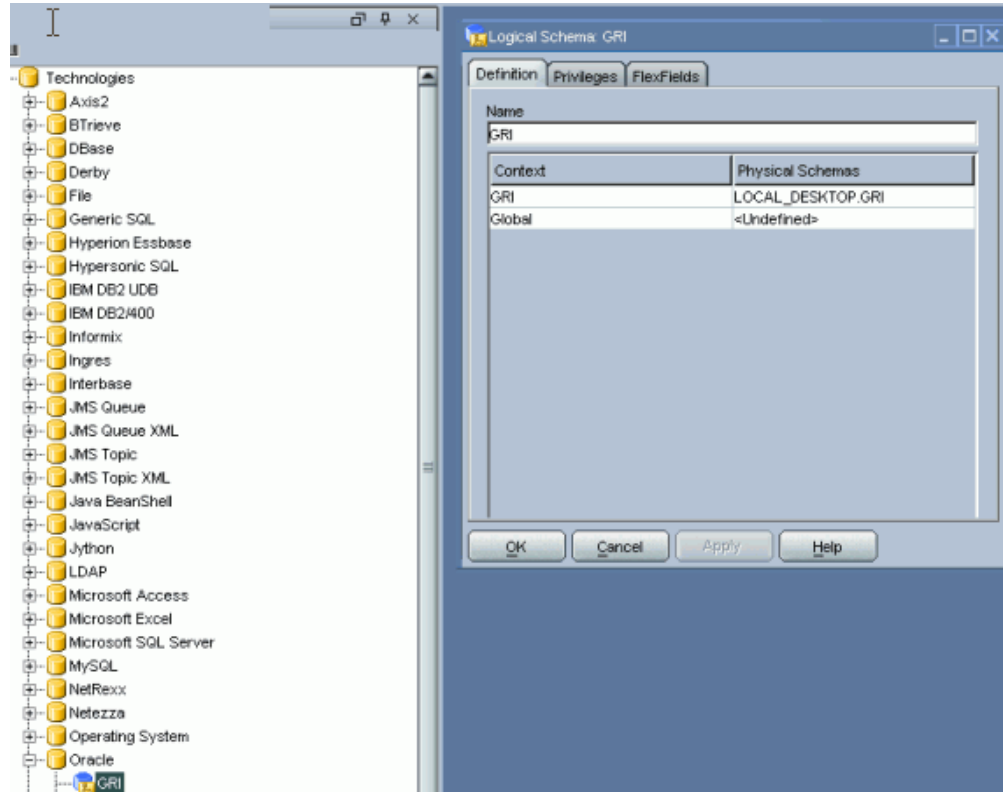
3. Create a Context:

In "Topology Manager", switch to the Context tab, and insert the new context (right click and insert context), as shown.



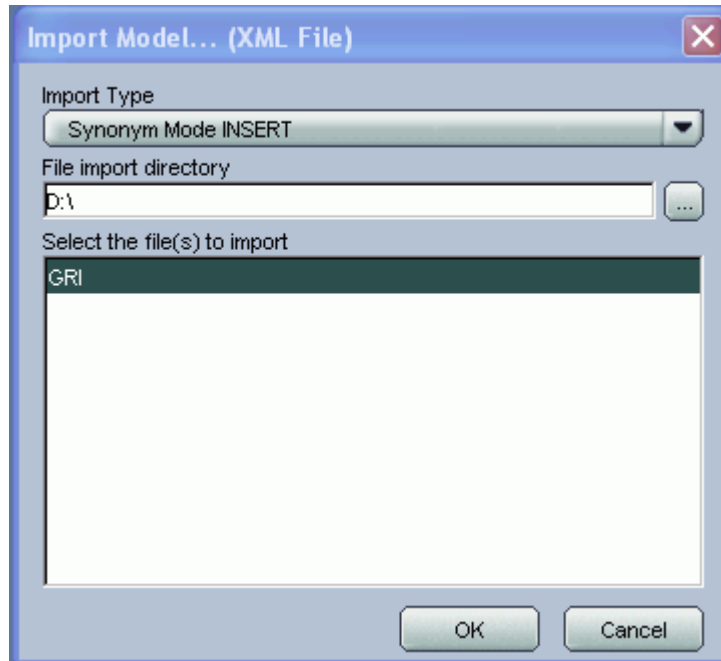
4. Create a Logical Schema:

In Topology Manager, switch to the "Logical Architecture" tab, under "Oracle Technologies" select "Insert Logical Schema", specify the name as "GRI" and choose the appropriate physical schema (created in Step 1) for the Context created (in Step 2).



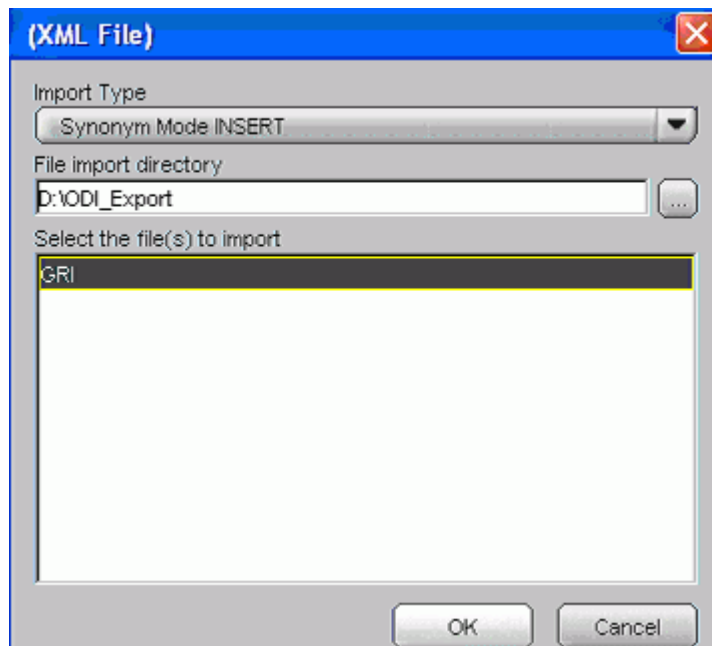
5. Import Model:

Login to Designer, right click on the Models tab. Select Import Model and import the .xml file supplied, as shown.



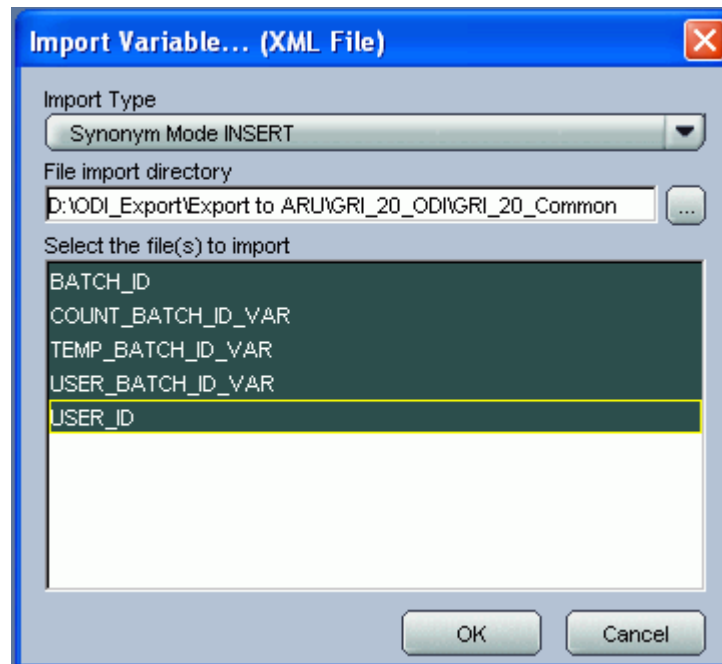
6. Import Project (without child components):

Import the Project file provided with the "INSERT" mode. The project file does not have any child components.



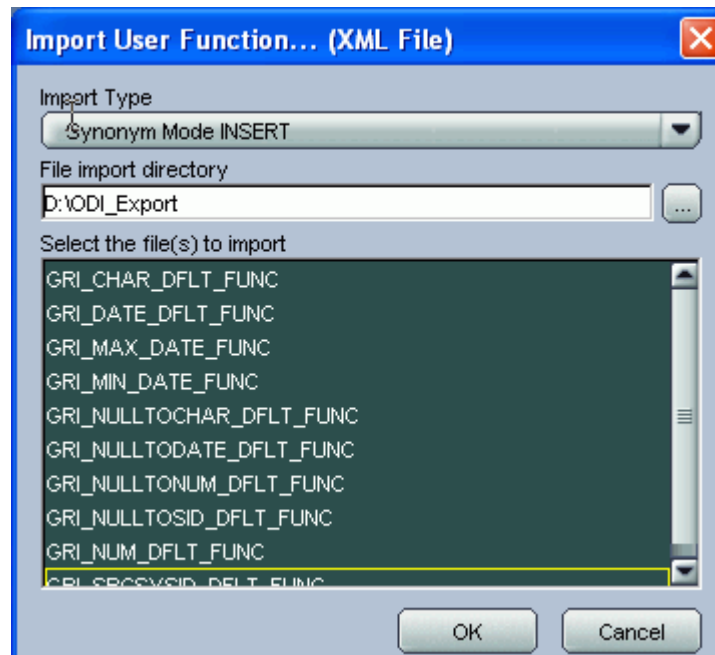
7. Import Project Variables:

Import the variables into the project with the "INSERT" option.



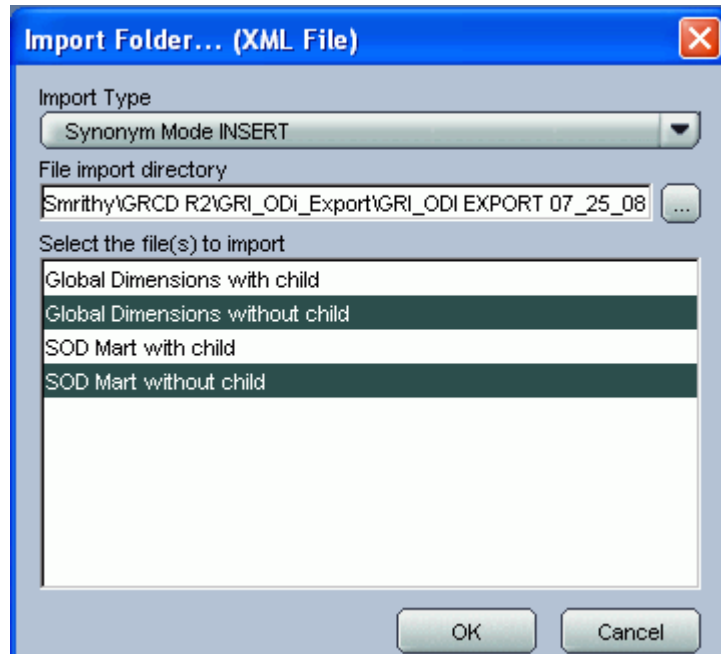
8. Import User Functions:

Import User Functions in the "INSERT" mode.



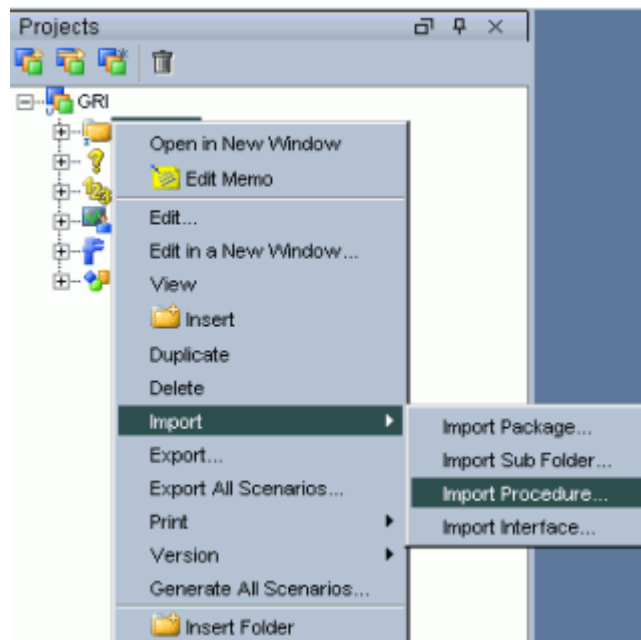
9. Importing Folders:

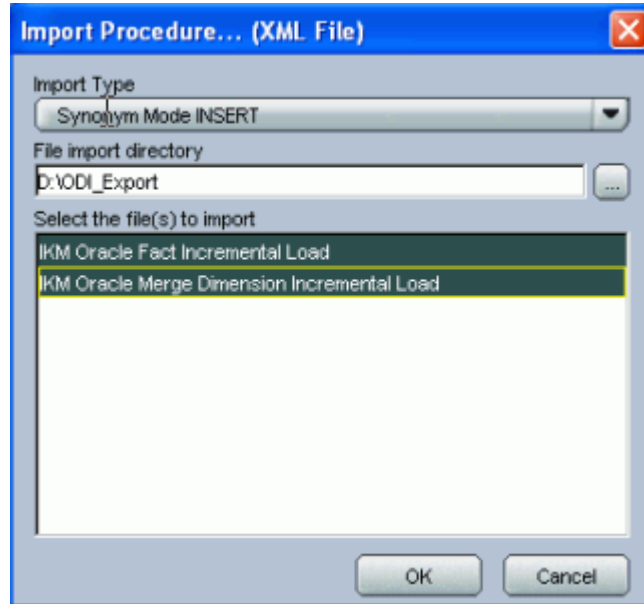
Import the Folders provided (SOD Mart and Global Dimensions) without the child component using "INSERT" mode.



10. Import Knowledge Modules:

Right click the imported SOD Mart folder, and select "Import Procedure".

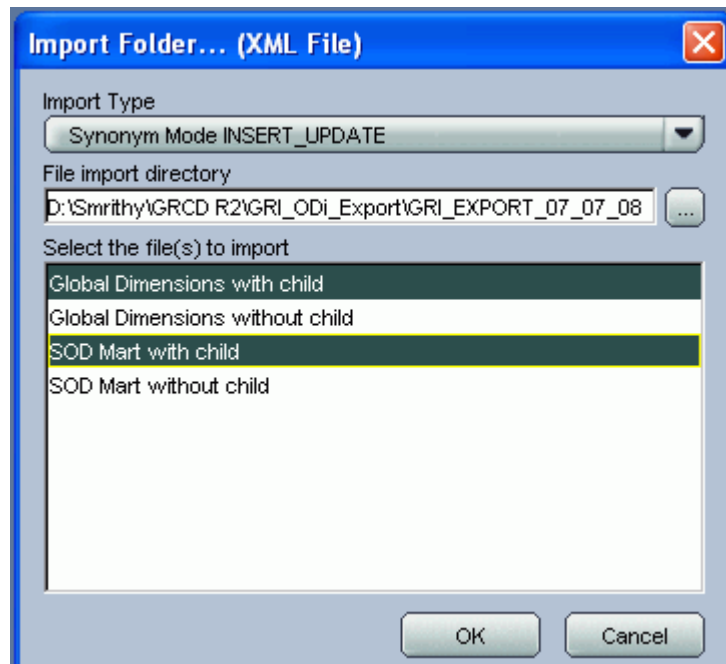




Import the "IKM Oracle Merge Dimension Incremental Load" and "IKM Oracle Fact Incremental Load" supplied, as shown above.

11. 11. Import Folders (with child components):

Import the folders (SOD Mart and Global Dimensions) with the "INSERT_UPDATE" option.



12. Once you are done importing, open the imported interface, and make sure that it does not show any errors.

Installing OBIEE Reports

The GRI_20_OBIEE.zip contains two zip files:

- GRCDiagnostic.zip
- GRCDWebcat.zip

These files contain the repository and web-catalog and are used in the following steps to install the repository and the reports-dashboards respectively.

1. After you successfully install OBIEE (OBIEE version 10.1.3.3.3), extract the delivered zip file GRCDiagnostic.zip. Place the GRCDiagnostic.rpd file in the C:\OracleBI\server\Repository folder.
2. In the C:\OracleBI\server\Config folder, edit the NQSConfig.INI file. Enter the name of the RPD file after "Star =" in the [REPOSITORY] section.
3. Place the GRCDWebcat.zip file in the C:\OracleBIData\web\catalog folder and unzip the file. The GRCDWebcat folder now appears in the Catalog folder.
4. In the C:\OracleBIData\web\config folder, edit the instanceconfig.xml file. Enter the path of the GRCDWebcat folder in between the <CatalogPath> tags.
5. Create the TNS entry to point to your GRCI schema in Oracle home directory.
6. Open the GRCDiagnostic.rpd in the Oracle BI Administration Tool and go to the Variable Manager under the Manage > Variables menu.
7. Update the GRI_DSN variable with the name of the TNS entry name.
8. Update the GRI_USER_ID with the database user ID.
9. Open the properties window for 'GRC Diagnostics > GRCI Connection Pool' in the Physical layer and provide the password for GRCI schema.
10. Save the changes in the Oracle BI Administration Tool.
11. Restart the Oracle BI Services.
12. Log into the OBIEE using this URL: <http://<localhost>:<TCPport>/analytics>, where <localhost> is the name of the machine or the IP address where OBIEE is installed, and <TCPport> is the Web Site TCP Port number.

13. The OBIEE login page loads.
14. The installation is now complete.

Security Integration with AACG (Optional)

This section describes the security integration between GRCI 2.0 and AACG 8.1.1 or later.

This section describes how a user logs into GRCI, and can drill-across to AACG to see more details without having to sign on.

Prerequisites

Installation of AACG version 8.1.1 and GRCI Release 2.0 is required.

Installed Software

- OBIEE (Oracle Business Intelligence Enterprise Edition) version 10.1.3.3.3 (with OC4J)
- Oracle HTTP Server (Apache 2.0)
- Web server and directory server. (Used here are SUN ONE Web server 6.1 and iplanet directory server 5.1)
- OAM (Oracle Access Manager) 10.1.4.0.1
- WebGate (OAM Web component) 10.1.4.0.1

For installing and setting up software, please refer to the installation and user guides. Web server and directory server must be installed prior to OAM installation, as it is a prerequisite for OAM installation. OAM is installed on some servers, and OBIEE, OHS (Oracle HTTP Server) and WebGate are installed on the client side.

Steps for Integration

Step 1. Configuring the Access System, Policy and Users in OAM

At least one Access Server must be installed and configured. A policy and AccessGate should be created for the resource you want to protect. At least one WebGate must be installed on the client side, and configured to communicate with the Access Server AccessGate function, and performance can also be configured to respond to their unique needs.

- In the access system configuration, set up the access server, host identifier, and the access gate.
- Login into Oracle Access Manager. Go to Access System Configuration -> Access Server Configuration -> Add In the access server, provide a name, host, port of the machine where OAM is installed, and the search parameters.

- Login into Oracle Access Manager. Go to Access System Configuration, on the side navigation pane, click Host Identifiers -> Add -> Specify a name, description and all possible identifiers for this host. As a host can be known by multiple names, the Host Identifiers feature is used to enter the official name for the host, and every other name by which the host can be addressed by users.

Create Access Gate. On the Access System Configuration page select Add New AccessGate. Provide a name, host, and port of the machine where OBIEE for GRCI is installed and other search parameters.

- Login into Oracle Access Manager. Go to Policy Manager -> Create Policy Domain -> Create a policy for the URL of the resource.

For each policy you create, you can assign a specific authentication scheme (Basic Over LDAP), an authentication rule, an authorization expression, and an auditing rule.

- Login into Oracle Access Manager. Go to Identity System Console -> User Manager Tab -> Create User Identity tab, and create a new user.

When the credentials are asked for to login into GRCI, a username and password should be entered. This will allow the user to drill down to AACG without having to log on.

- Below are the steps that describe the flow of the OAM component:
 - a) User attempts to access web resource (http) on OHS which is protected by Oracle Access Manager, a request is received by WebGate
 - b) WebGate requests the policy from the Access Server to see if the resource (URL) is protected or not
 - c) If the resource/URL is not protected, the user is returned to the previous page. If resource/URL is protected, WebGate will ask the user to authenticate
 - d) Credentials entered by the user, and are validated against the LDAP directory via the access system
 - e) After successful authentication, a Oracle Access Manager Single Sign-On cookie is sent to the user's browser

Note: Refer to Oracle® Access Manager Access Administration Guide (10.1.4.2.0) for more details.

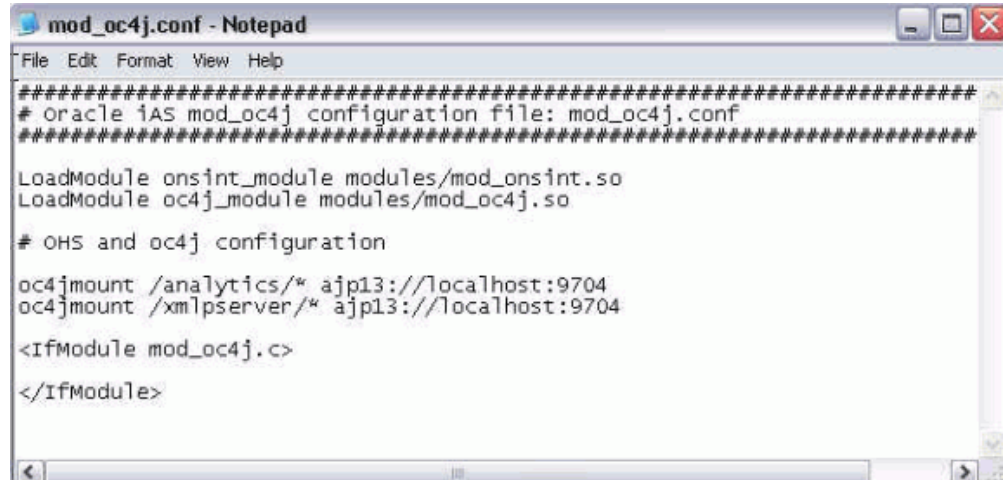
Step 2. Configuring mod_oc4j for Accessing an Application deployed in OC4J

- The directive Oc4jMount is used to make an Application deployed to OC4J accessible through OHS via mod_oc4j. This directive can be included in the file mod_oc4j.conf.

Update mod_oc4j.conf located in C:\OraHome\ohs\conf directory

Add the following lines:

```
# OHS and oc4j configuration
oc4jmount /analytics/* ajp13://localhost:9704
```

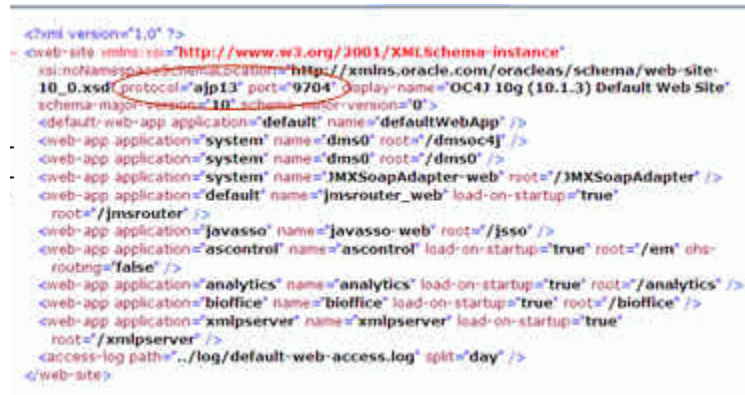


- Restart the OPMN process by running ons.exe from C:\OraHome_3\opmn\bin.

Communication between OHS and OC4J uses Apache JServ protocol AJP13

Update protocol="ajp13" in

C:\OracleBI\oc4j_bi\j2ee\home\config\default-web-site.xml



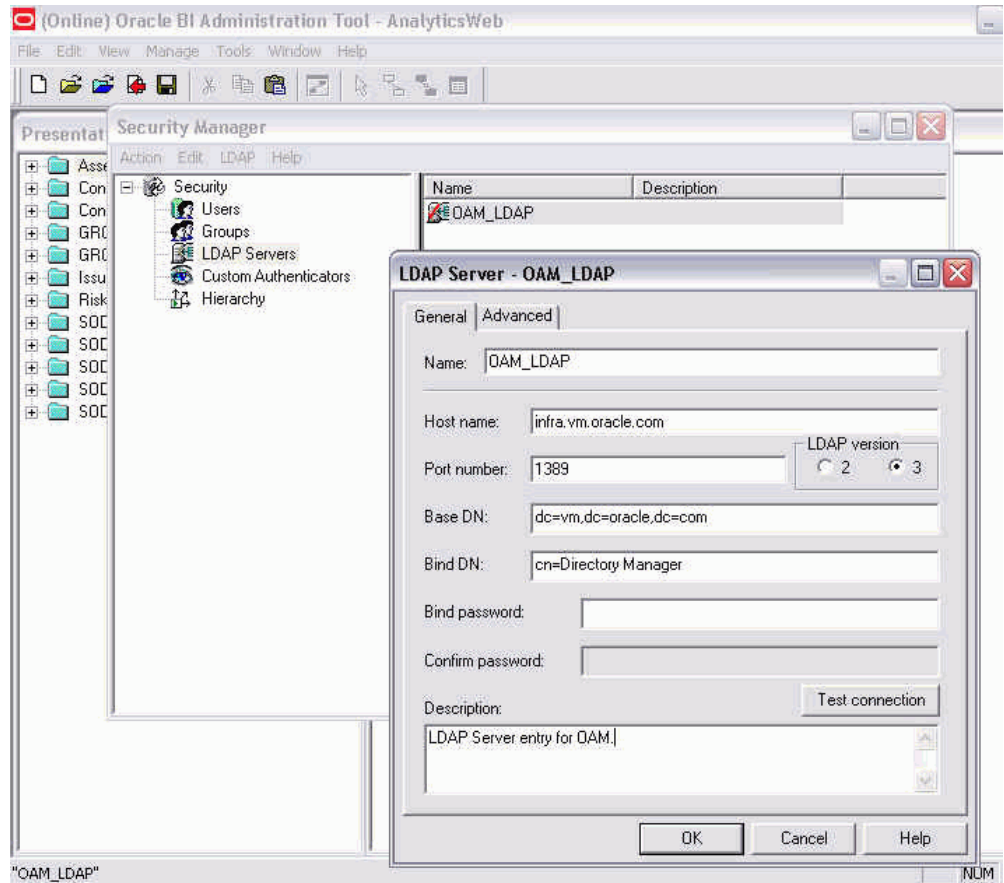
Step 3. OBIEE - LDAP Authentication

Create a new LDAP Server entry in the repository (rpd) for iplanet Directory where OAM users get stored using the following procedure.

a) To Modify the Repository for User Authentication in iplanet Directory

- Open the rpd in the BI Administration Tool and select Manage > Security from the application menu.

- From the Security Manager menu, choose Action > New > LDAP Server.
- In the General tab, enter values for fields as shown in the following example:
Hostname = < iplanet Directory hostname>
Port number = < iplanet Directory port>
LDAP version = LDAP 3
Base DN = < Base distinguished name (DN)>
Bind DN = < Distinguished name required to bind to iplanet Directory >
Bind password = < Password of bind DN>
where the Base DN field identifies the starting point of the authentication search.
If the Bind DN and Bind password entries are blank, anonymous binding is assumed.



- Return to the General tab and click on the Test Connection button to ensure the connection to iplanet Directory server is successful.

b) Configuring the Initialization Block Used for User Authentication

- One initialization block is required for user authentication and to configure it to use LDAP authentication. It will set the value of USER system session variable.
- Create new init block
- In the Session Variable Initialization Block window, click on the "Edit Data Source" button. Select LDAP as the Data Source Type from the drop-down and select the LDAP Server that was created in above step.
- Select the Edit Data Target button. In the System Session Variable window, enter "USER" in the Name field. Click OK. Click OK when asked to confirm if you want to use this name.
- Test the authentication by clicking on the Test button in the Session Variable Initialization Block window.

c) Configuring the Initialization Block Used to set the GROUP for the User

Note: OBIEE will be not able to recognize nor use any LDAP defined user-to-group relationships until 11g (or later).

Users are typically assigned to groups via an OBIEE repository session init block using an external source (E.g. a database table) that contains the user-to-group association. This init block sets the GROUP session variable.

- Shutdown Oracle BI Server and Oracle BI Presentation Server services
- Launch Oracle BI Administration tool. Open the rpd file in offline mode
- From the Manage menu, click on Variables to launch the Variable Manager
- From the menu click on Action, Select New and choose Session->Initialization Block to create an initialization block

- In the Data Source section, click on Edit Data Source. From the Data Source Type drop-down box and choose Database. In the 'Default Initialization String' window type the following SQL:

```
SELECT ROLE_NAME
FROM GRCD_USERS A, GRI_D_ROLE_USER_BG B, GRI_D_ROLE_TL C
WHERE A.USERNAME=':USER' AND
A.SRC_SYS_ID='AG80'
AND A.GRCD_USER_SID = B.GRCD_USER_SID
AND A.SRC_SYS_ID = B.SRC_SYS_ID
AND B.ROLE_SID = C.ROLE_SID
AND B.SRC_SYS_ID = C.SRC_SYS_ID
AND C.LANGUAGE = 'VALUEOF(NQ_SESSION.LANGUAGE_CODE)'
```

- The Connection Click on Browse to launch the Select Connection Pool window. Click on the appropriate Connection Pool and click Select, then click OK.
- In the Variable Target section, click on Edit Data Target. Click New to launch the Session Variable window. In the name box enter GROUP. Click OK. Accept the 'special purpose' prompt by clicking on Yes.
- Enable the 'Required for Authentication' check box.
- Save the initialization block.

d) Creation of Repository Group and Presentation Catalog Group

Create a repository group and a presentation catalog group (the same as group that was assigned in the prior step). For example, if the GROUP has a variable set to Apps Administrator, then the user creates a repository group, and a presentation catalog group as "Apps Administrator". This step is needed in order to see the group in the rpd and the webcat to further secure presentation layer catalogs, dashboards, folders and answers. A dynamic assignment is done in the prior steps only.

Note: Creation of a group should be done by logging in as an Administrator to rpd and webcat. This should be done on a different machine that does not have OAM integration on it. With OAM integration only, OAM users can log into presentation services even if they don't have Administrator user privileges.

- **Creation of Repository Group**

Open the GRCM rpd in the OBIEE Administration tool and logon with admin privileges

Click on Manage->Security from the menu

On the Security Manager window, select Groups in the left pane and click on Action->New->Group. Enter a group name that gets assigned to the GROUP session variable in the prior step.

- **Creation of a Presentation Catalog Group**

Connect to OBIEE Presentation server and log on as Administrator

Click on Settings->Administration, select 'Manage Presentation Catalog Groups and Users', and click on 'Create new catalog group'

Enter the group name that gets assigned to the GROUP session variable in the prior step, Dashboard Name and Dashboard Builder columns of the Create Catalog Group screen

Note: Check Oracle® Business Intelligence Enterprise Edition User Guide for securing presentation layer catalogs, dashboards, folders and answers.

Step 4. Configuring BI Presentation Services to Use the Impersonator User

The steps to configure BI Presentation Services are:

a) Creating the Oracle BI Server Impersonator User

- Open the BI Server repository file (.rpd) using BI Administration Tool.
- Select Manage > Security to display the Security Manager.
- Select Action > New > User to open the User dialog box.

Enter a name and password for this user.

For example, Name = Impersonator and Password = secret.

- Click OK to create the user.

Make this user a member of the group Administrators.

- Double-click on the icon for the user that was created.
- In the Group Membership portion of the dialog box, check the Administrators group.

b) Creating Adding Impersonator User Credentials to Oracle BI Presentation Services Credential Store

1. Open a command prompt window or command shell on the machine where BI Presentation Services has been installed.
2. Navigate to the directory OracleBI/web/bin.
3. Execute the CryptoTools utility to add the impersonator user credentials to the BI Presentation Services Credential Store:

```
cryptotools credstore -add -infile OracleBIData/web/config/credentialstore.xml
```

4. Supply values for the prompted parameters, as shown:

```
C:\OracleBI\web\bin>cryptotools credstore -add -infile C:/OracleBIData/web/config/credentialstore.xml
>Credential Alias: impersonation
>Credential "impersonation" already exists. Do you want to overwrite it? y/n (y) : y
>Username: Impersonator
>Password: password
>Do you want to encrypt the password? y/n (y): y
>Passphrase for encryption:password123
>Do you want to write the passphrase to the xml? y/n (n): n
>File "C:/OracleBIData/web/config/credentialstore.xml" exists. Do you want to overwrite it? y/n (y): y
```

c) Configuring Oracle BI Presentation Services to Identify Credential Store and Decryption Passphrase

Step 1. Locate the node within the instanceconfig.xml file.

Step 2. Specify the attribute values as shown in the following example.

If the node does not exist, create this element with sub-elements and attributes with attribute values given in the following example.

```

<WebConfig>
  <ServerInstance>
    <!-- other settings ... -->
    <CredentialStore>
      <CredentialStorage type="file" path="<path to credentialstore.xml>" passphrase="<passphrase>"/>
    <!-- other settings ... -->
    </CredentialStore>
  <!-- other settings ... -->
</ServerInstance>
</WebConfig>

```

After modification, CredentialStore node in instanceconfig.xml file looks as below:

```

<?xml version="1.0"?>
<WebConfig>
  <ServerInstance>
    <!-- other settings ... -->
    <CredentialStore>
      <CredentialStorage type="file" path="C:/OracleBIData/web/config/ credentialstore.xml" passphrase="password123"/>
    <!-- other settings ... -->
    </CredentialStore>
  <!-- other settings ... -->
</ServerInstance>
</WebConfig>

```

d) Configuring BI Presentation Services to Operate in the OAM Environment

1. Open instanceconfig.xml for editing. Locate the <Auth>element. If this does not exist, create this element, sub-elements and parameters as shown in the following example:

```

<!-- other settings ... -->
<Auth>
  <SSO enabled="true">
    <ParamList>
      <!-- IMPERSONATE param is used to get the authenticated user's username and is
      required
      -->
      <Param name="IMPERSONATE" source="httpHeader" nameInSource="SSO_UID" />
    </ParamList>
  </SSO>
</Auth>

```

2. Secure the machines that are permitted to communicate with BI Presentation Services directly.

This can be done by setting the Listener\Firewall node in instanceconfig.xml with the list of HTTP Server or servlet container IP addresses. For example:

```

<Listener>
<Firewall>
<Allow address="127.0.0.1"/>
<Allow address="10.111.111.111"/>
</Firewall>
<!-- other settings ... -->
</Listener>

```

Step 5. Drilldown to source system from OBIEE

- GRI_S_SRC_SYSTEM_INFO table is used to store the source instance URL and component path. SOURCE_URL column stores URL and policy, conflictpath id store component path for policy and conflict path respectively. Refer to AACG documentation for populating data for these three columns.
- Create an Initialization Block and Dynamic Repository Variable, which are used to create the URL for the source system. For every drill to page, a separate Init Block creation is required.
 1. In OBIEE Admin tool open the rpd. Go to Manage->Variables->Action->New->Repository Initialization Block.
 2. In the Repository Variable Init Block window put init block name.
 3. Click on edit data source write a query to get URL and component from GRI_A_SRC_SYSTEM_INFO table. For conflictpathId drill down the query would look like the following:

```

SELECT SOURCE_URL || CONFLICT_COMPONENT
FROM GRI_A_SRC_SYSTEM_INFO
WHERE SRC_SYS_ID = 'AG80'

```

- Assign a connection pool for this init block. Test the authentication by clicking on the Test button in the Repository Variable Initialization Block window.
- Select Edit Data Target button. Select New in Repository Variable Init Block Variable Window. Create a Dynamic Repository variable. Similarly, an Init block for policy Id should be created.
Similarly, Init block for policyID should be created.
- Create a logical column in the business layer of the OBIEE admin tool and select the check box for Use existing logical columns as source. Specify the expression from which the logical column should be derived. Replace the :1 with the dynamic field value, for multiple parameters use nested REPLACE functions. For example, the expression for logical column for conflictpathId drill would look like the following:

Logical Column - Conflict Path ID Link

General | Data Type | Aggregation | Levels

Name:

Belongs to Table:

Sort order column:

☒ Use existing logical columns as the source

Description:

- Create an answer with the logical column as created above and change the data format as HTML) and run the report.
- "Save system-wide column formats" and "Save Content with HTML Markup" privilege should be given to Everyone, which is by default given to Presentation Server Administrators

References

1. Oracle Access Manager Installation Guide 10g (10.1.4.0.1)
2. Oracle Access Manager Identity and Common Administration Guide10g (10.1.4.0.1)
3. Oracle Access Manager Access Administration Guide 10g (10.1.4.0.1)
4. Oracle Business Intelligence Infrastructure Installation and Configuration Guide
5. Oracle Business Intelligence Enterprise Edition User Guide

Installation and Upgrade Options for Oracle Fusion Governance, Risk and Compliance Intelligence 2.0

Overview

This chapter refers the user to the previous sections of the GRCI 2.0 installation guide when installing for both GRCM 7.8 and AACG 8.1.1 or later.

Additionally within this chapter, if there is an existing GRCI 1.0 installation and it needs to be upgraded to GRCI 2.0, then the user should refer to the upgrade section, and follow the instructions.

Installing Oracle Fusion Governance, Risk and Compliance Intelligence for both GRCM 7.8 and AACG 8.1.1 or Later

Installing Oracle AACG Scripts

Please refer to Chapter 3, which describes the necessary steps for the installation of AACG 8.1.1 or later as a source application.

Installing Oracle GRCM Scripts

Please refer to Chapter 2, which describes the necessary steps for the installation of GRCM 7.8 as a source application.

Installing ODI Code

Please refer to Chapter 3, which describes the necessary steps for the installation of ODI Code in GRCI.

Installing OBIEE Reports

Please refer to Chapter 2, which describes the necessary steps for the installation of OBIEE Reports.

Multi-Language Setup for OBIEE

Please refer to Chapter 2, to view the source language files required to support multiple languages in OBIEE

Installing BI Publisher Reports

Please refer to Chapter 2, for instructions on installing Oracle BI Publisher 10.1.3.3.3 and data source configuration.

Security Integration with GRCM 7.8

Please refer to Chapter 2, which provides optional details and requirements on the integration of the security components for both GRCM 7.8 and GRCI 2.0.

Security Integration with AACG 8.1.1

Please refer to Chapter 3, which provides optional details and requirements on the integration of the security components for both AACG 8.1.1 or later and GRCI 2.0.

Upgrading GRCI 1.0 to GRCI 2.0

Overview of GRCI 1.0 Data Load

This section applies to users who are upgrading from GRCI 1.0 to GRCI 2.0. The source of GRCI 1.0 is solely GRCM, and the data is loaded in a 'truncate-load' fashion. This means that during every load cycle, data in the GRCI tables are truncated and reloaded from the source application (GRCM). However, if a user wishes to drop, recreate the tables, and reload them from the source application, they are able to pass a value of 1 to the vForceCreate parameter, which would then drop all the objects, recreate them and then reload them.

Upgrading GRCI 1.0 to GRCI 2.0

In order to upgrade from GRCI 1.0 to GRCI 2.0, users can follow the approach of recreating the entire schema and reloading it from the source, by using the vForceCreate as explained.

The parameter's value is set in the file Execute_Create.sql to 1, and when it is set to 1, all the GRCI objects are recreated and reloaded.

After setting this variable, refer to Chapter 2 if GRCM 7.8 is the only source application; or, refer to the beginning of this chapter if both GRCM 7.8 and AACG 8.1.1 are the sources.

The sections on installing Oracle Scripts contains detailed instructions on the installation and configuration of the model, ETL and Reports-Dashboards components of GRCI 2.0.

Please read the note section in "Creating the Target Physical Model" in Chapter 2 for further information about the upgrade of GRCD_TIME_D, GRCD_TIME_TL and GRCD_USERS.

ETL Execution

This appendix covers the following topics:

- Execution Sequence
- ETL Execution
- Execute a Package

Execution Sequence

Order of Execution for the ETL:

The following packages are placed into a single package (GRI_MASTER_PKG).

1. GRI_DIMENSIONS_PKG
2. GRI_BRIDGE_TABLES_PKG
3. GRI_FACTS_PKG

The order for execution of the Dimensions is as follows:

1. GRI_INSTANCE_PKG
2. GRI_GENERIC_DIM_PKG
3. GRCD_USER_MAIN_PKG
4. GRI_POLICY_PKG
5. GRI_ENTITLEMENT_PKG
6. GRI_ACCESS_POINT_PKG
7. GRI_APPS_USER_PKG

8. GRI_D_RUN_PKG
9. GRI_EXCLUSION_PKG

Steps 4-8 may be run independent of each other, but the rest should be run in numeric order.

The bridge tables can be run independent of each other, and these are the packages present in the GRI_BRIDGE_TABLES_PKG. They should be run after the loading of all the dimensions.

1. GRI_D_ROLE_USER_BG_PKG
2. GRI_D_ROLE_USER_BG_PKG
3. GRI_POLICY_DETAIL_BG_PKG
4. GRI_D_ENTLMNT_GENERIC_DIM_BG_PKG
5. GRI_D_ENTITLEMENT_AP_BG_PKG

The GRI_FACTS_PKG contains the following packages for loading the conflicts and conflict paths and they should be loaded in the following order and only after the loading of the dimensions and bridge tables.

1. GRI_F_CONFLICTS_T_PKG
2. GRI_D_POLICY_PREV_RUN_BG_PKG
3. GRI_F_CONFLICT_PATH_T_PKG
4. GRI_F_CONFLICT_PATH_T_PKG_2

ETL Execution

In the ODI Designer module, (N) GRI > SOD Mart > Packages; the user can then locate the following master package: GRI_MASTER_PKG.

The dimension and bridge table related interfaces and packages are found by navigating in the ODI Designer module to (N) GRI > SOD Mart.

The fact table and related interfaces and packages are found by navigating in the ODI Designer module to (N) GRI > SOD Mart > Facts.

There are three ETL Execution options:

Option 1:

1. Execute GRI_MASTER_PKG Package.

2. This action triggers all the packages required to load the entire star schema.

Option 2:

Important: Execute the packages in the following order.

1. GRI_DIMENSIONS_PKG – this package will load all the dimension tables.
2. GRI_BRIDGE_TABLES_PKG – this package will load all the bridge tables.
3. GRI_FACTS_PKG – this package will load all the fact tables.

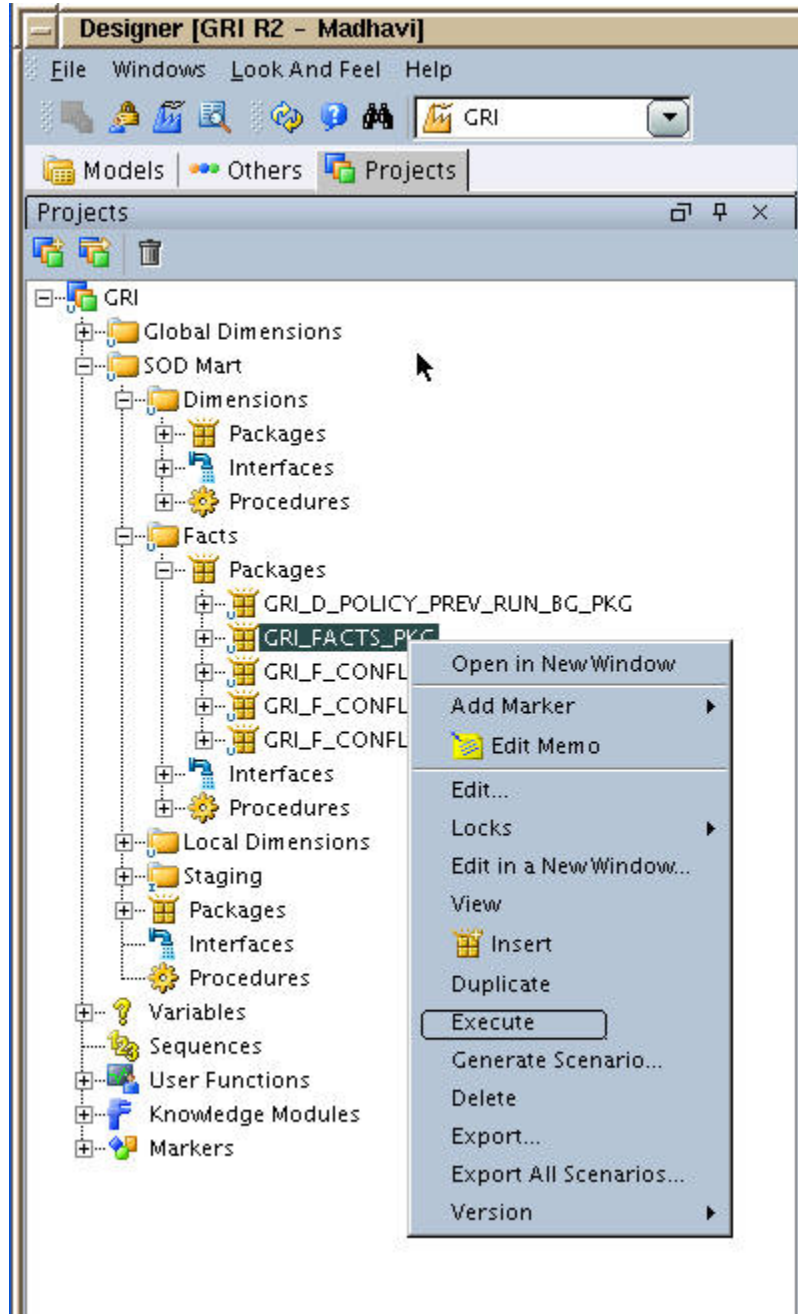
Option 3:

Run individual table level packages, in the same order as in **Option 2**.

Execute a Package

In order to execute a package, navigate to the ODI Designer and locate the required package to execute

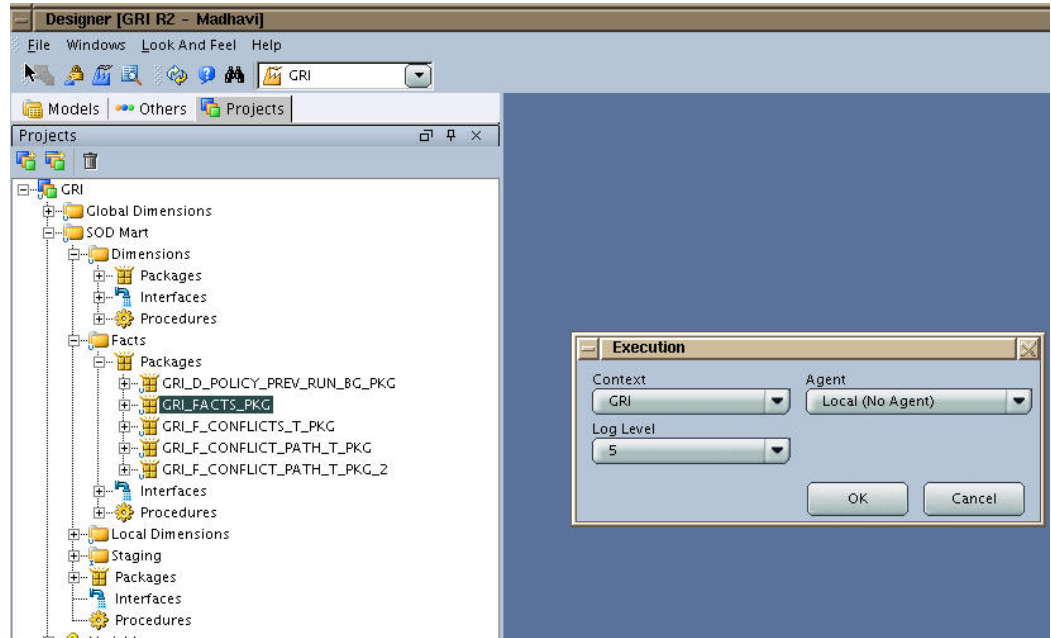
Right click on that package, and then click Execute as shown below:



In the Execution window, select the context that was created as part of the ODI Code installation.

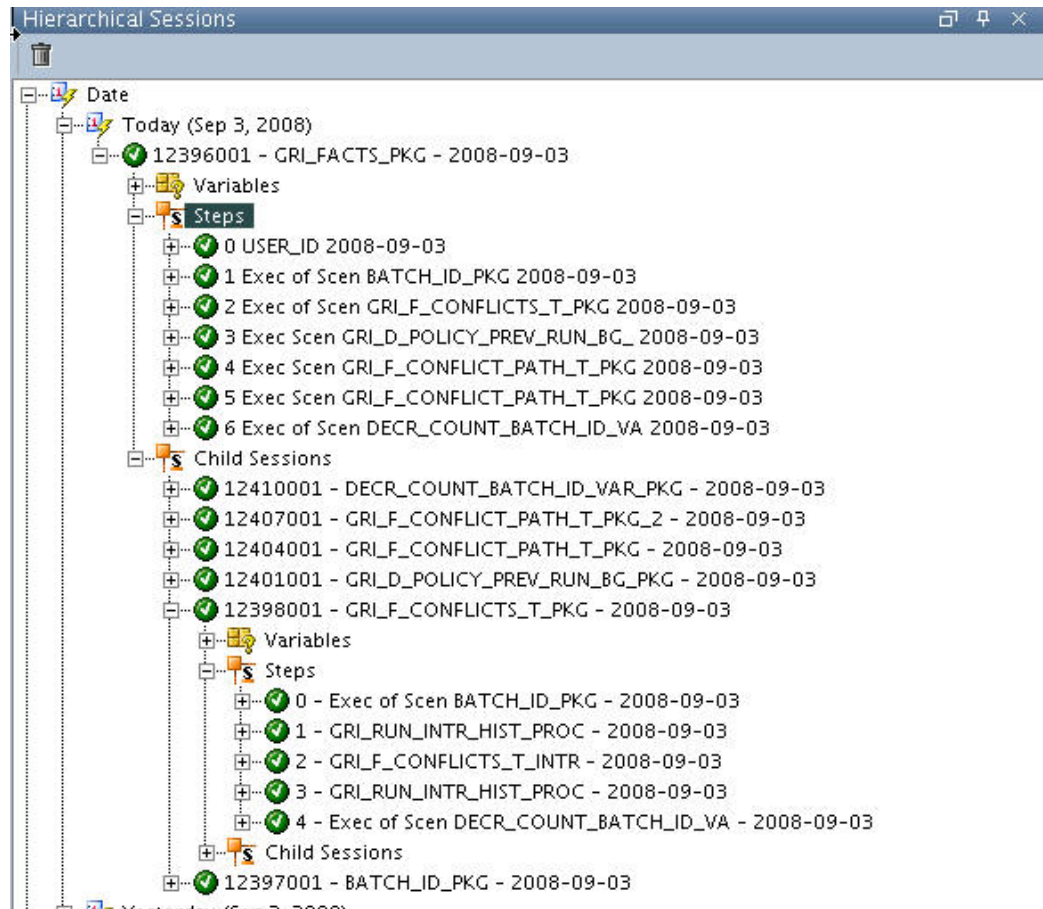
Note: Please refer to Chapter 3 "Installing ODI Code"

Click OK. This starts a session for the executed package.



The status of a session and its corresponding steps and tasks can be checked in, in the ODI Operator module.

In case of a higher-level package, such as one encapsulating multiple child packages, the status for each child package session can also be monitored.



Verify that the package has run successfully. The result of each task execution can be viewed in the Execution tab of Session Task window.

Verify the number of rows processed as part of each task in the session.

Note: Please refer to the Oracle Data Integrator User's Guide for more detail on using the ODI Designer and ODI Operator modules.

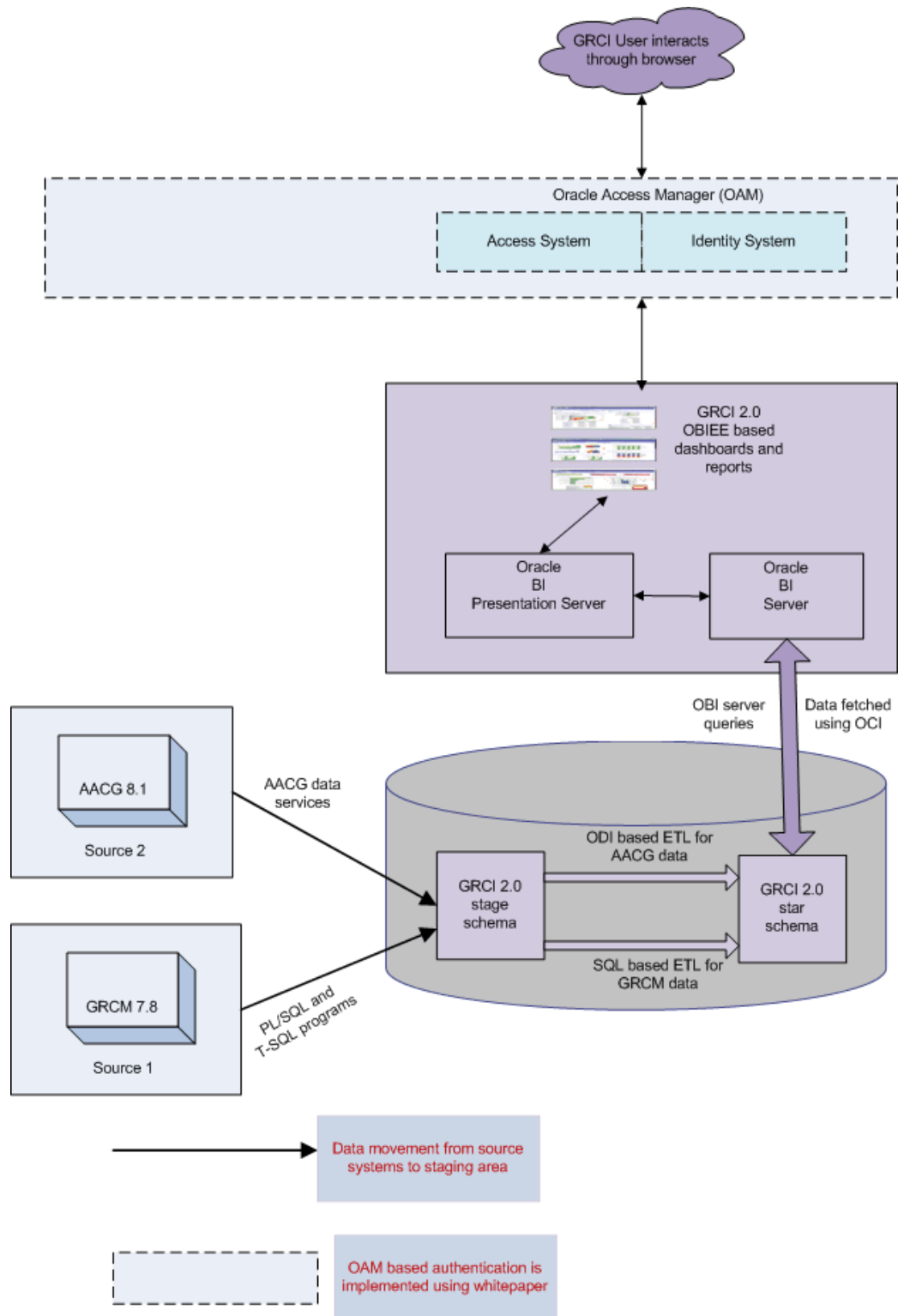
B

Architecture

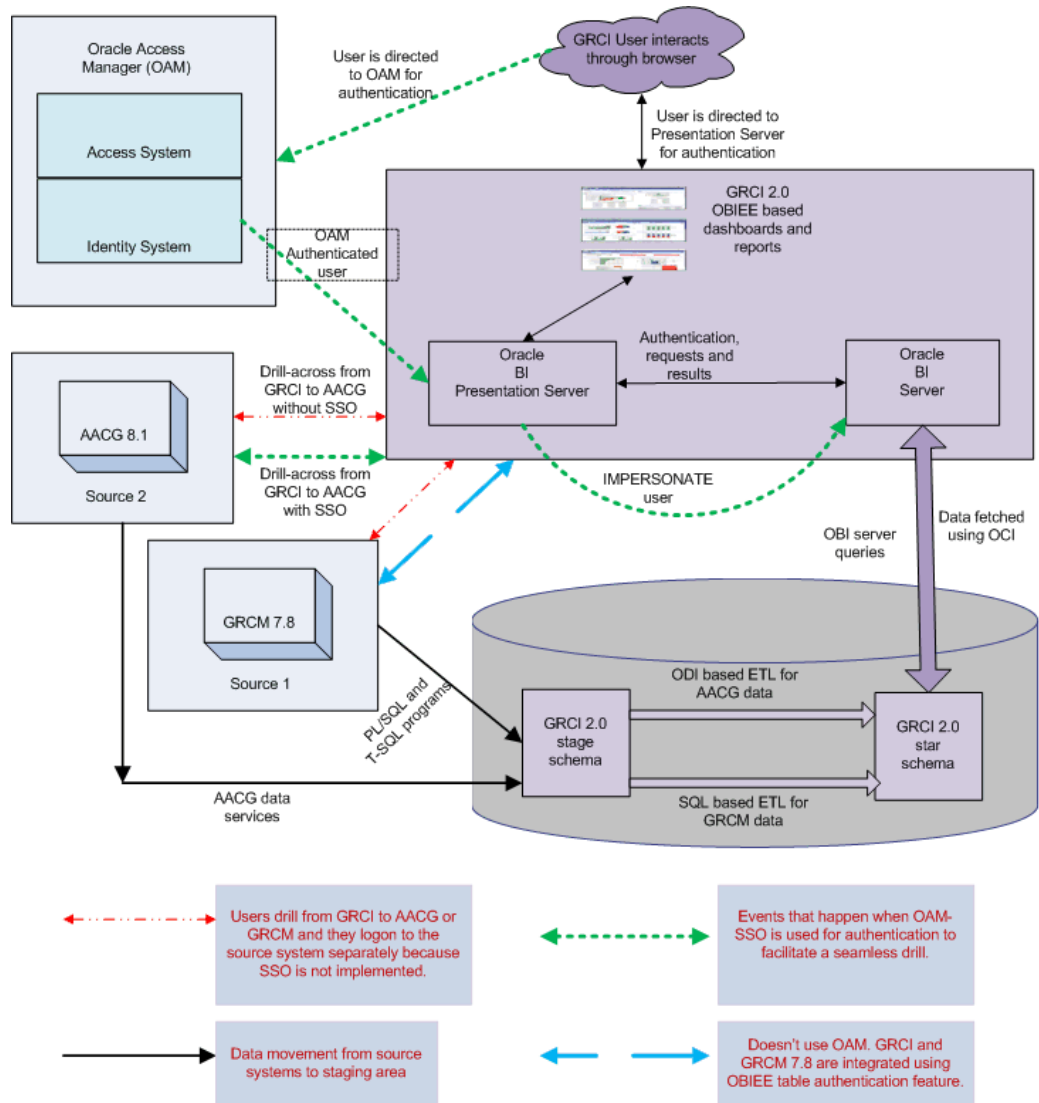
This appendix covers the following topics:

- Data Flow Diagram
- Detailed Data Flow Diagram

Data Flow Diagram



Detailed Data Flow Diagram



Logical and Physical Models

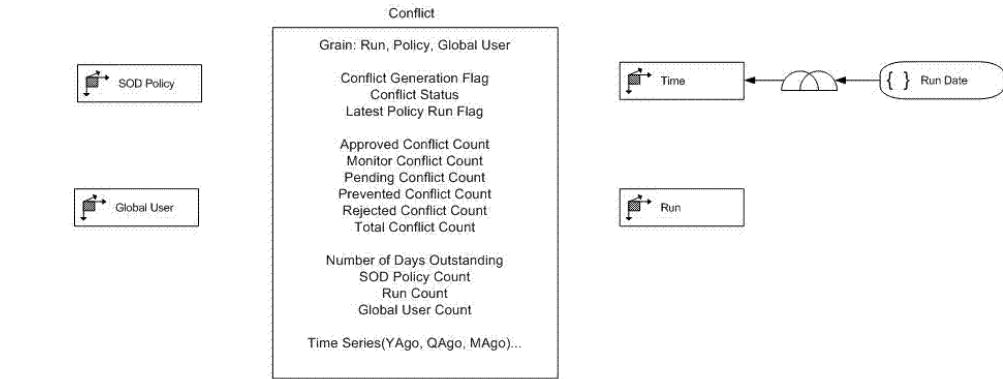
This appendix covers the following topics:

- Data Flow Diagram
- GRCI - AACG 8.1.1 or later Logical Model
- GRCI - AACG 8.1.1 or later Physical Model
- GRCI - GRM 7.8 Logical Model
- GRCI - GRM 7.8 Physical Model

Data Flow Diagram

GRCI - AACG 8.1.1 or later Logical Model

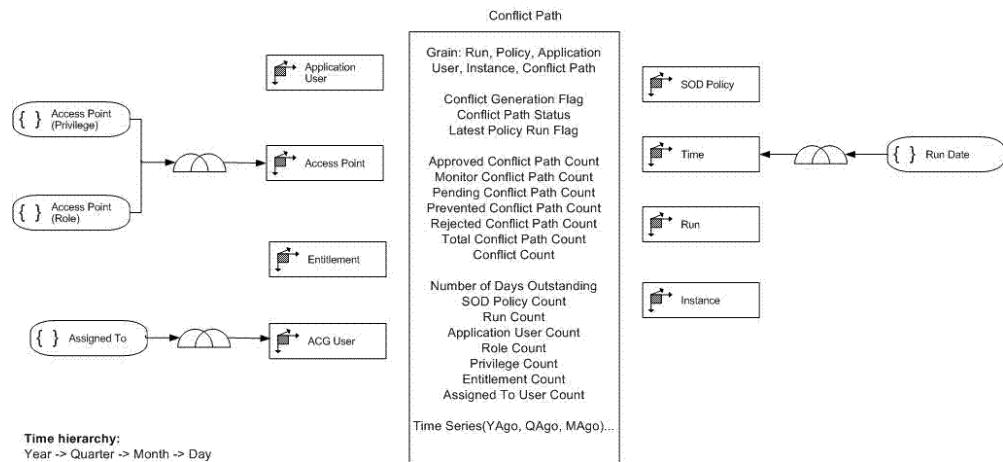
- Conflicts



Time hierarchy:
Year -> Quarter -> Month -> Day

Policy hierarchies:
Policy Type -> Policy Name
Policy Priority -> Policy Name
Process -> Policy Name
Risk -> Policy Name

- Conflict Path

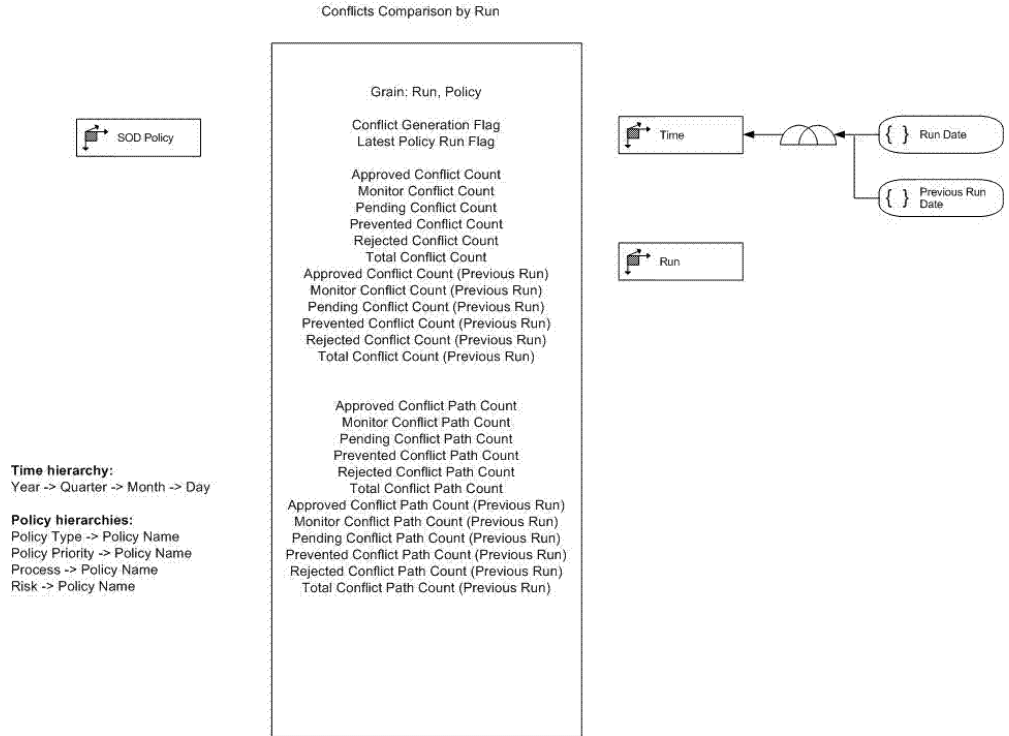


Time hierarchy:
Year -> Quarter -> Month -> Day

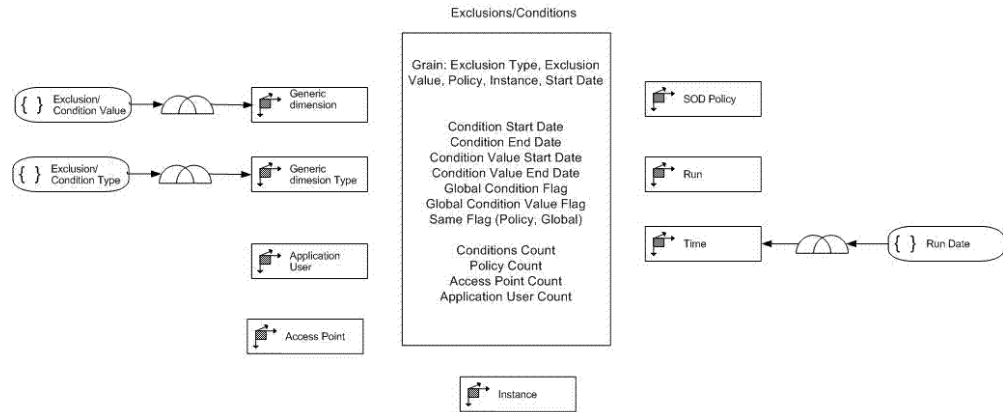
Policy hierarchies:
Policy Type -> Policy Name
Policy Priority -> Policy Name
Process -> Policy Name
Risk -> Policy Name

Access Point hierarchy:
Access Point Type -> Access Point Name

- Conflict comparison by Run



- Exclusions

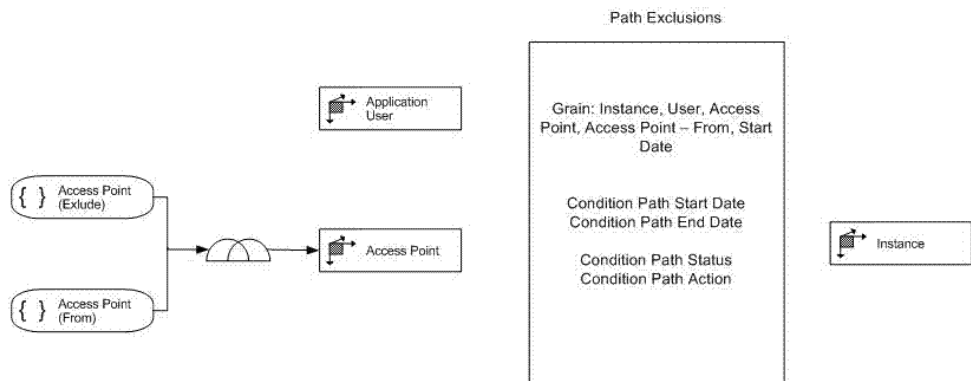


Time hierarchy:
Year -> Quarter -> Month -> Day

Policy hierarchies:
Policy Type -> Policy Name
Policy Priority -> Policy Name
Process -> Policy Name
Risk -> Policy Name

Access Point hierarchy:
Access Point Type -> Access Point Name

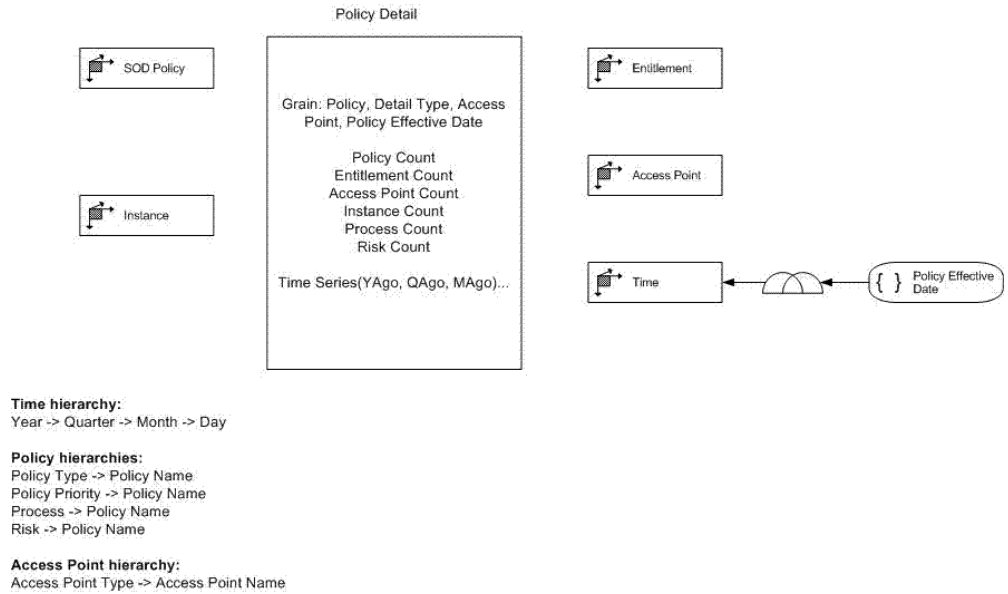
- Path Exclusion



Policy hierarchies:
Policy Type -> Policy Name
Policy Priority -> Policy Name
Process -> Policy Name
Risk -> Policy Name

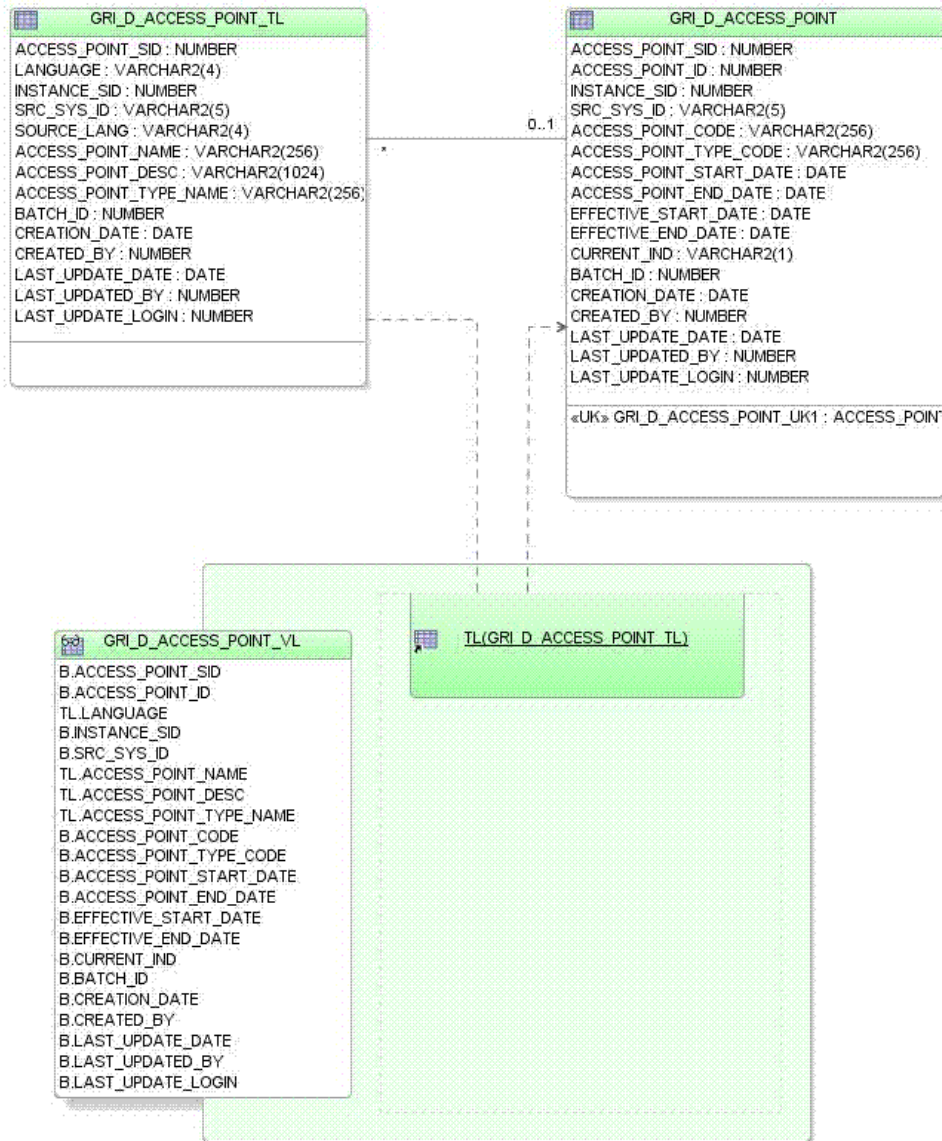
Access Point hierarchy:
Access Point Type -> Access Point Name

- Policy Detail

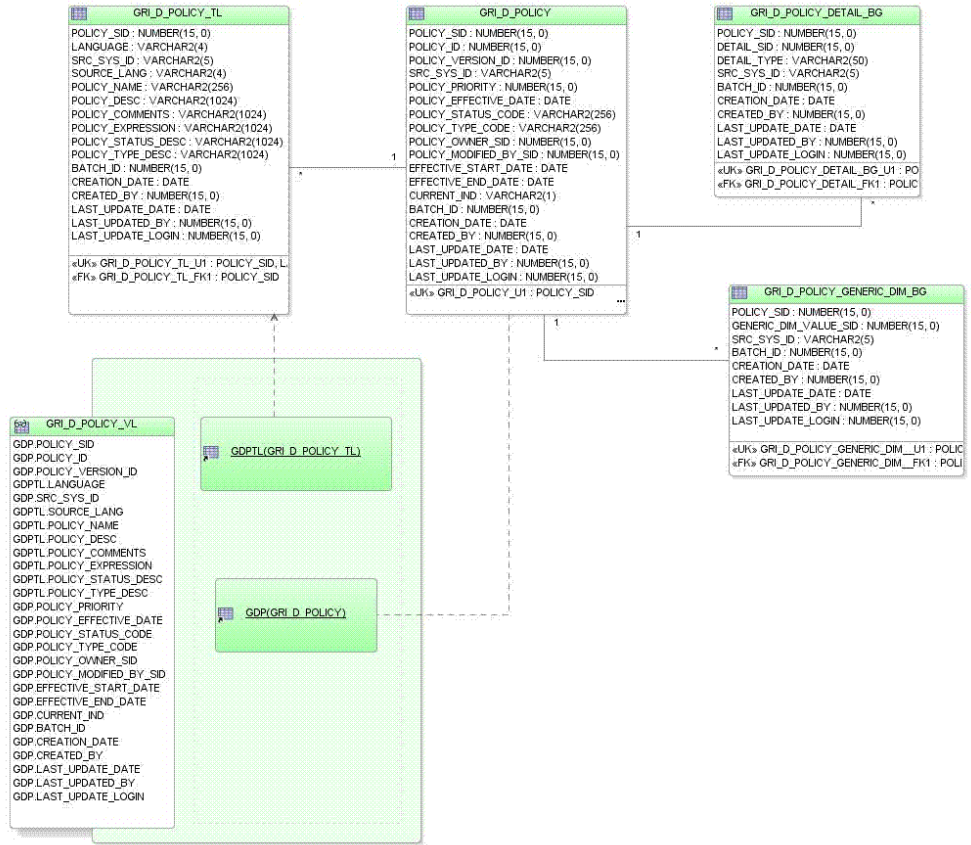


GRCI - AACG 8.1.1 or later Physical Model

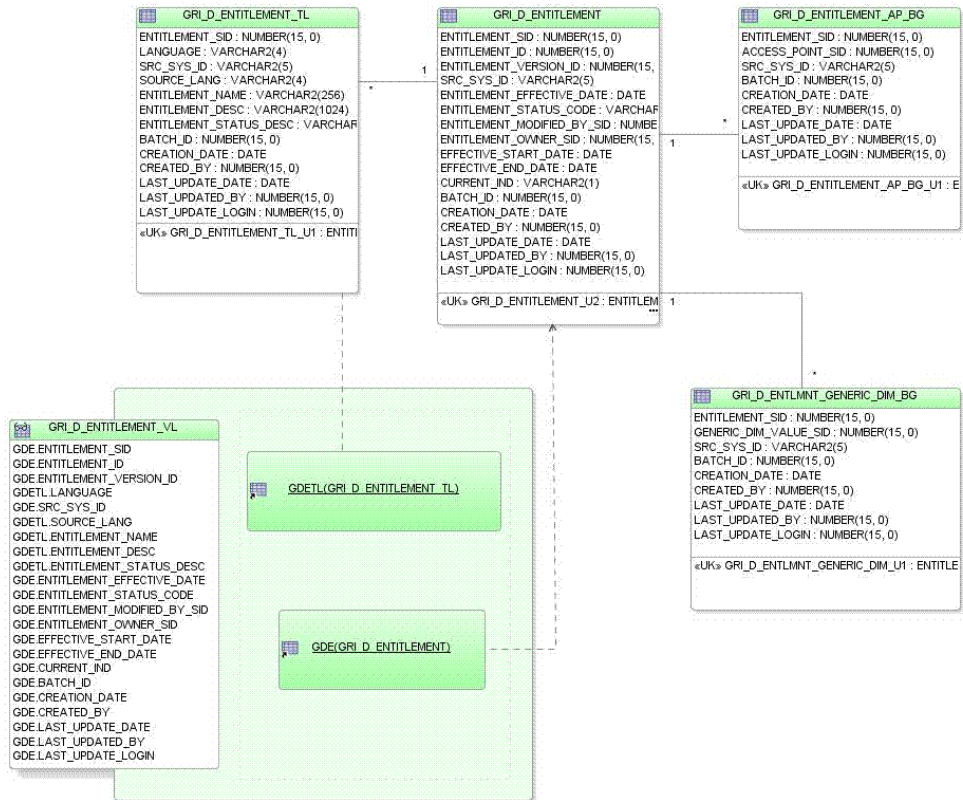
- Access Point



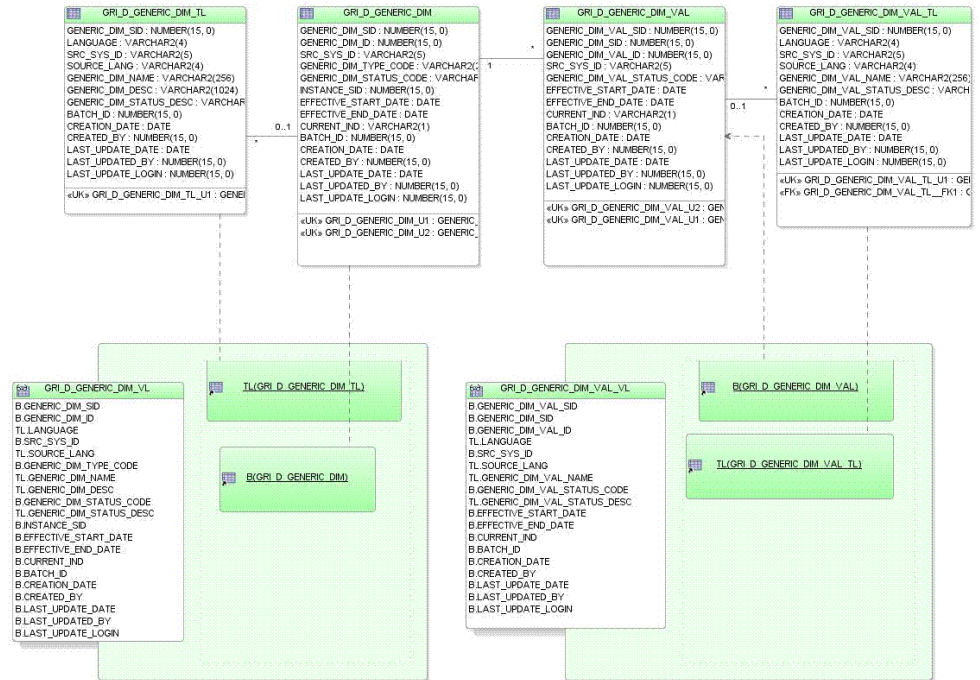
- Policy



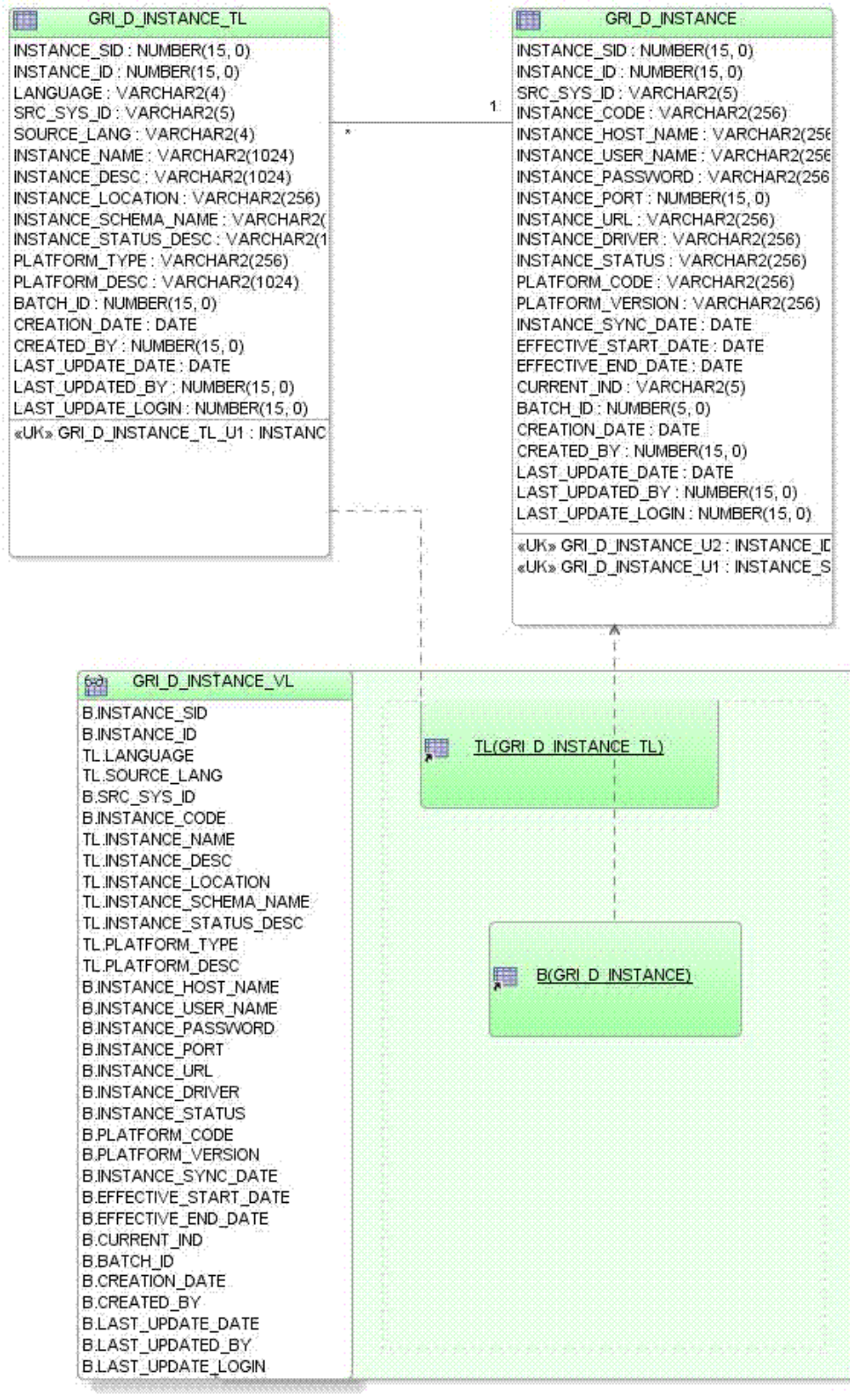
- Entitlement



- Generic Dimension



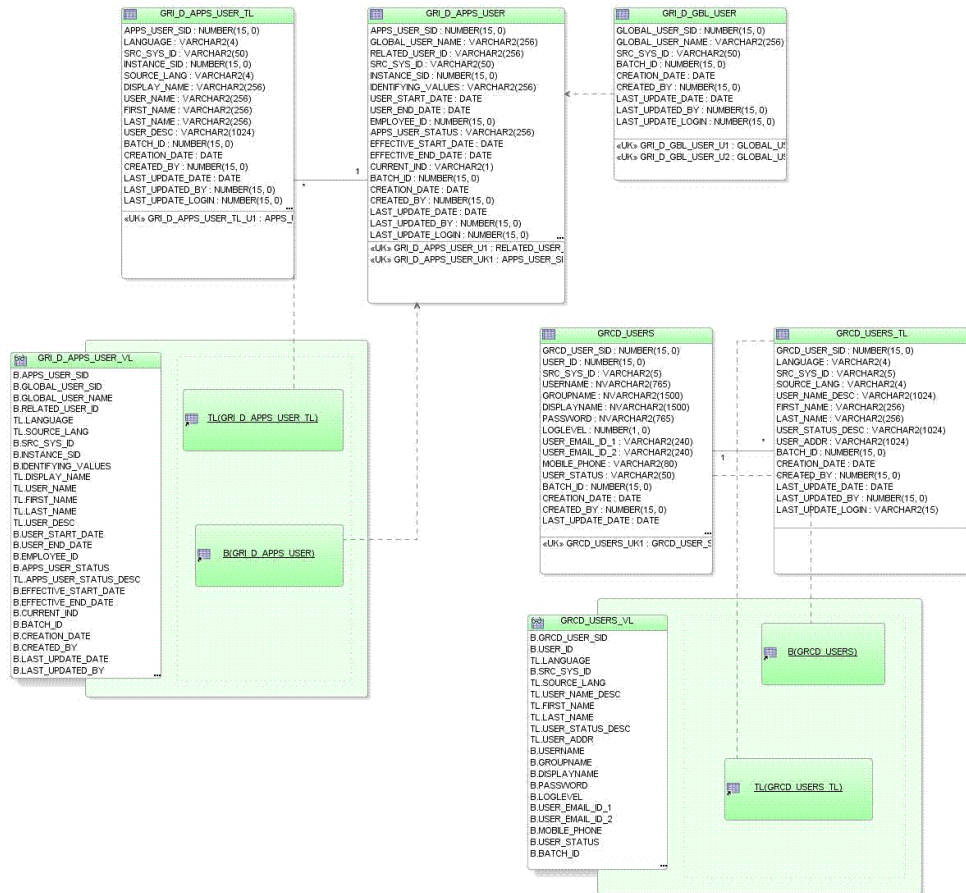
- Instance



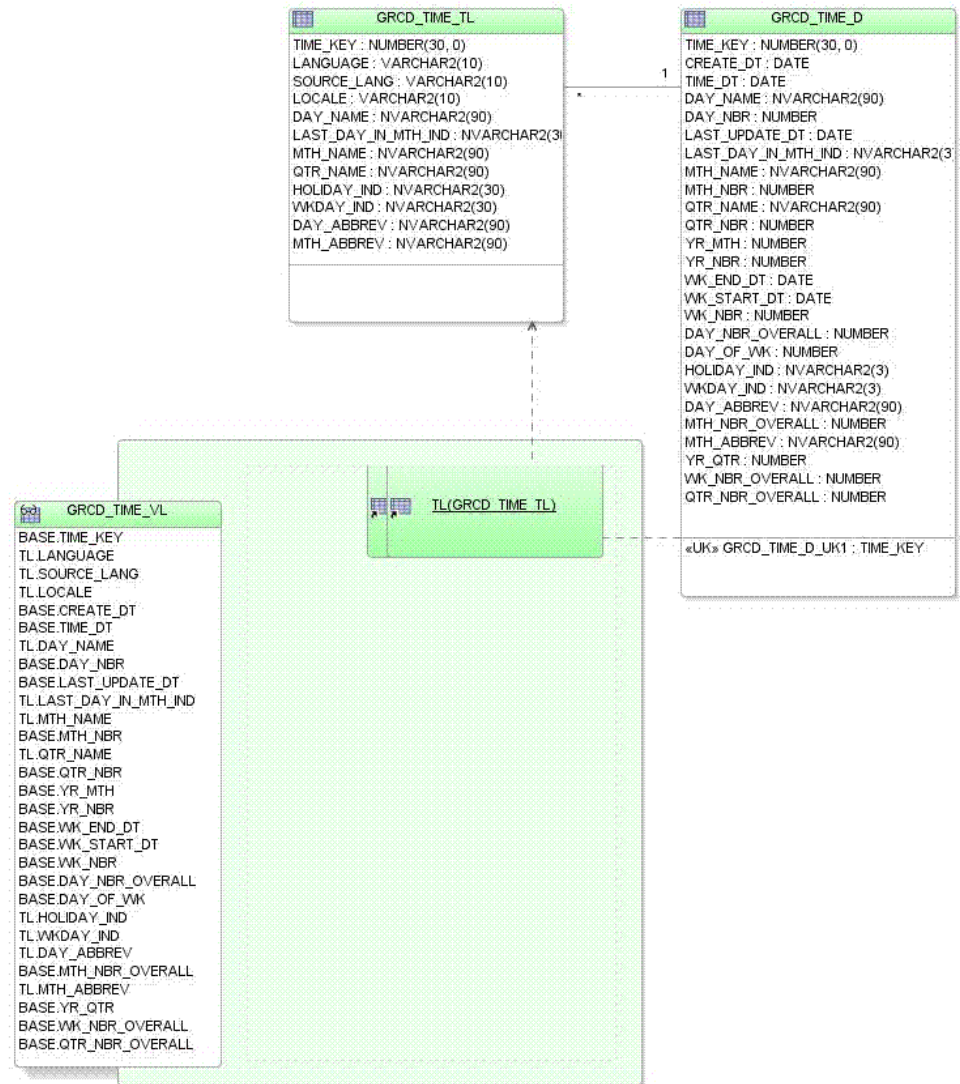
- Run

GRI_D_RUN	
RUN_SID	NUMBER(15, 0)
SRC_SYS_ID	VARCHAR2(50)
RUN_ID	NUMBER(15, 0)
RUN_DATE_SID	NUMBER(15, 0)
TOTAL_CONFLICTS_CNT	NUMBER(15, 0)
TOTAL_CONFLICT_PATH_CNT	NUMBER(15, 0)
RUN_END_DATE	DATE
EFFECTIVE_START_DATE	DATE
EFFECTIVE_END_DATE	DATE
CURRENT_IND	VARCHAR2(1)
BATCH_ID	NUMBER(15, 0)
CREATION_DATE	DATE
CREATED_BY	NUMBER(15, 0)
LAST_UPDATE_DATE	DATE
LAST_UPDATE_LOGIN	NUMBER(15, 0)
LAST_UPDATED_BY	NUMBER(15, 0)
«UK» GRI_D_RUN_U1 : RUN_SID	
«UK» GRI_D_RUN_U2 : RUN_ID, SRC_SYS_ID	

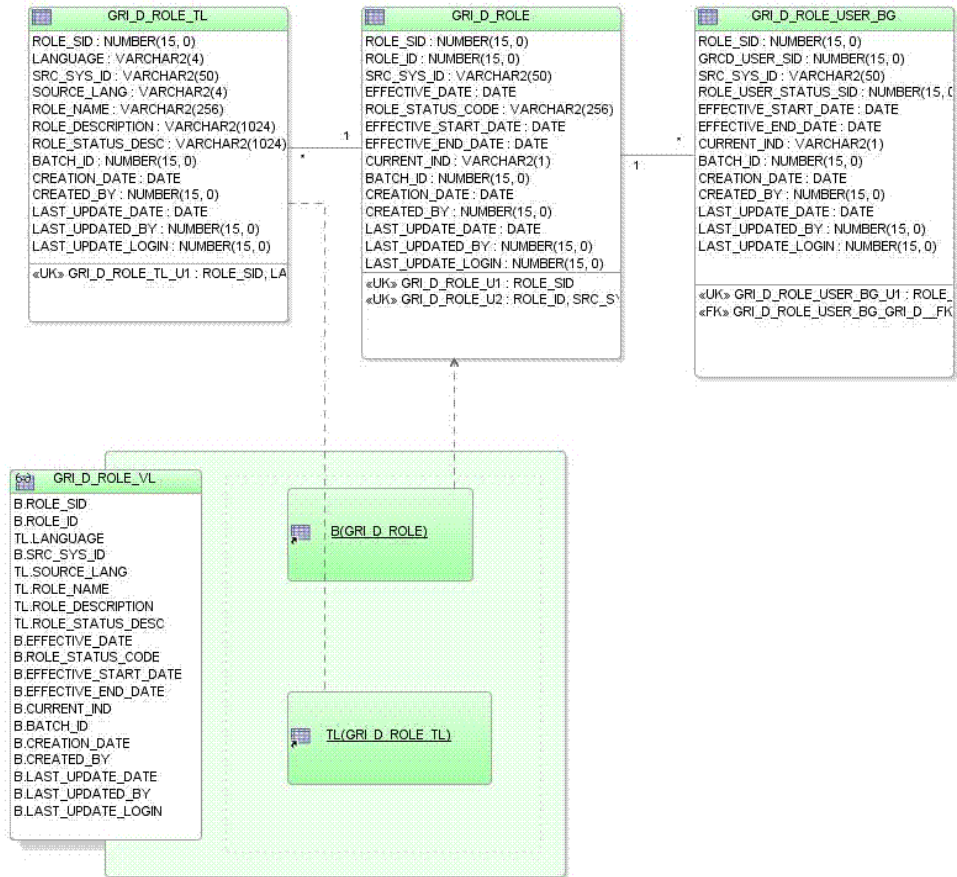
- User



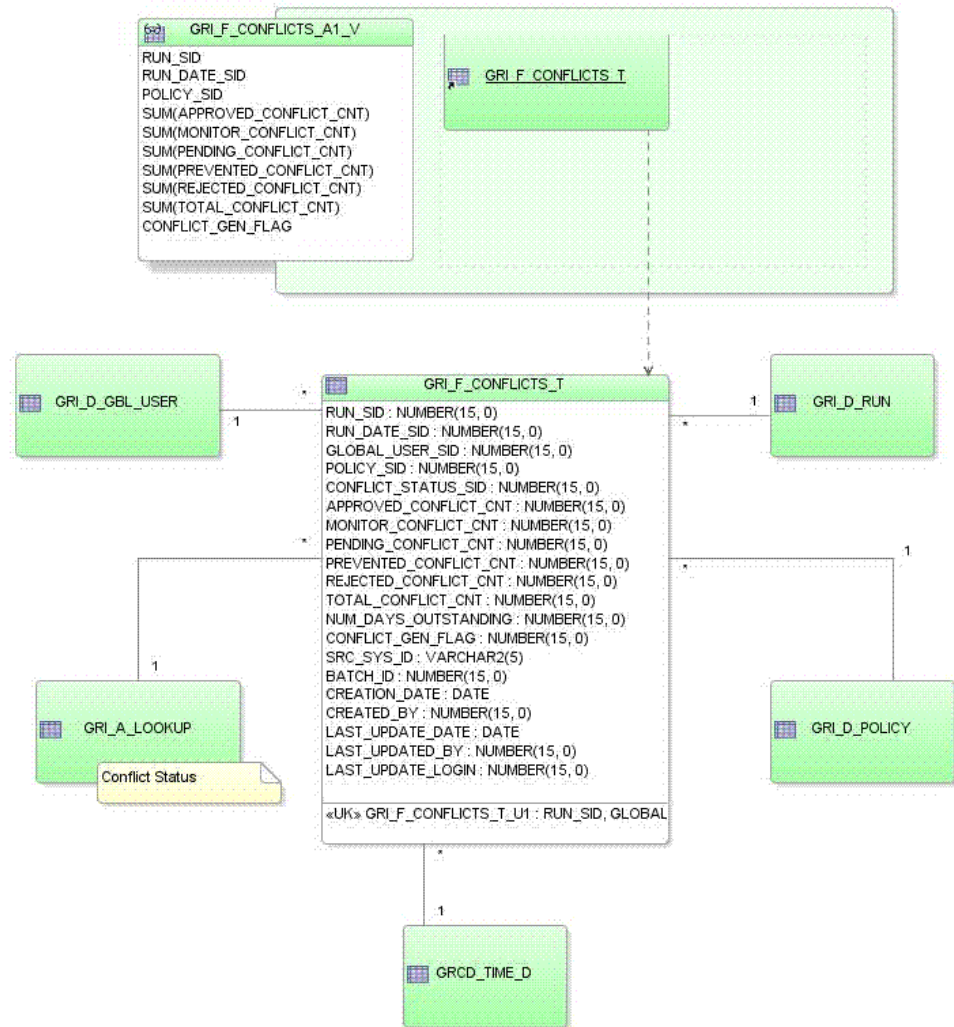
- Time



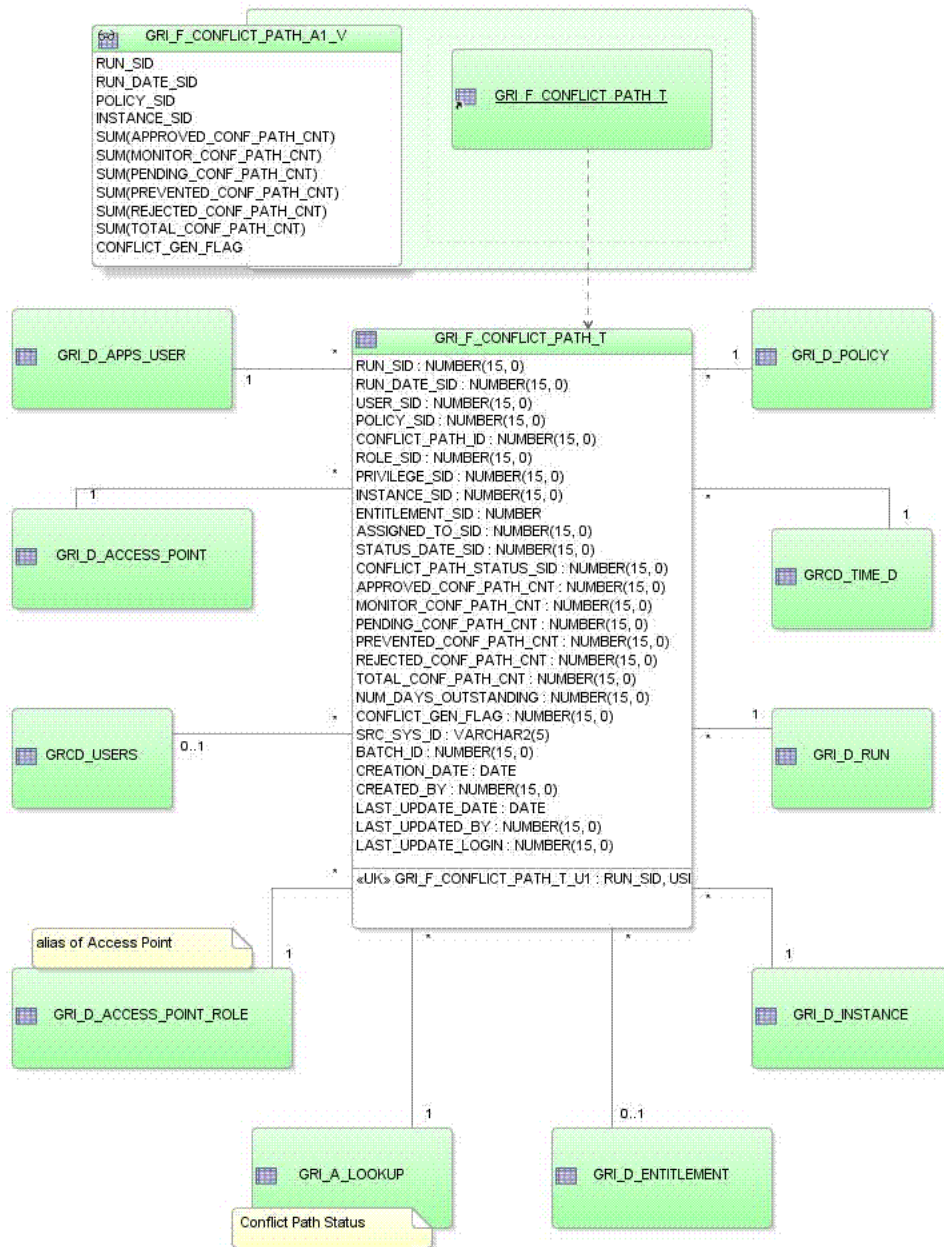
- AG Role



- Conflicts Star



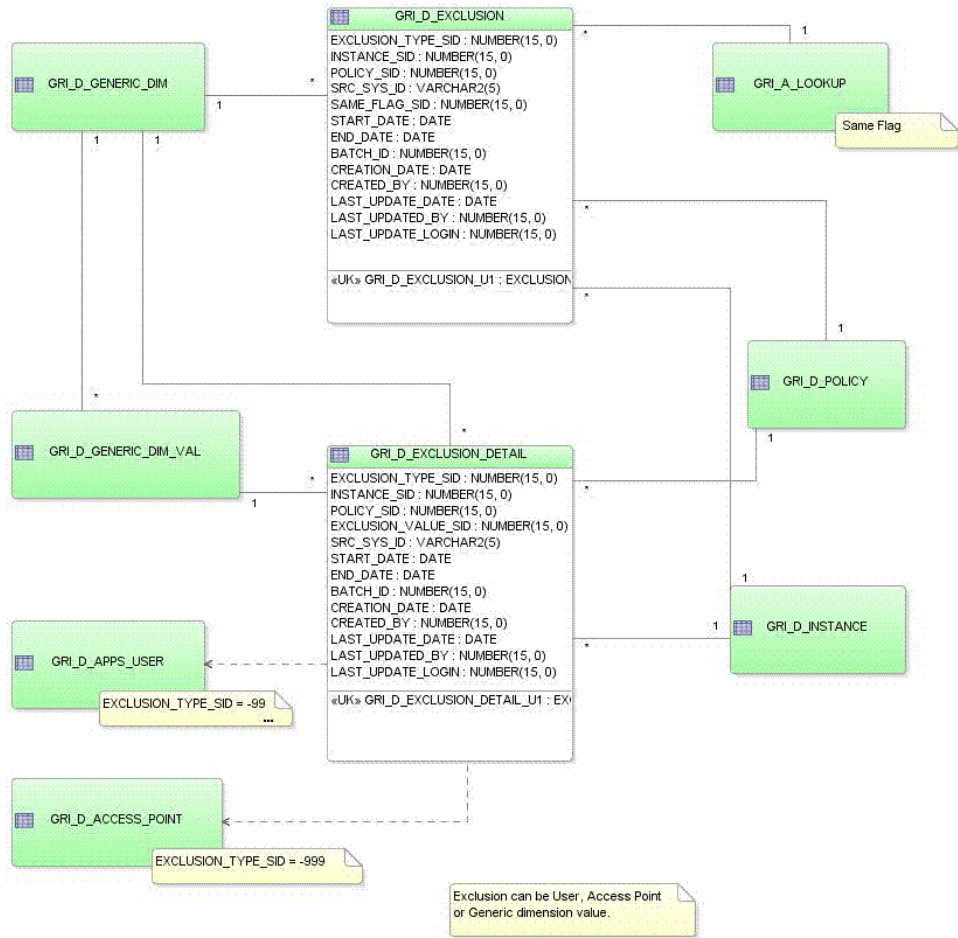
- Conflict Path Star



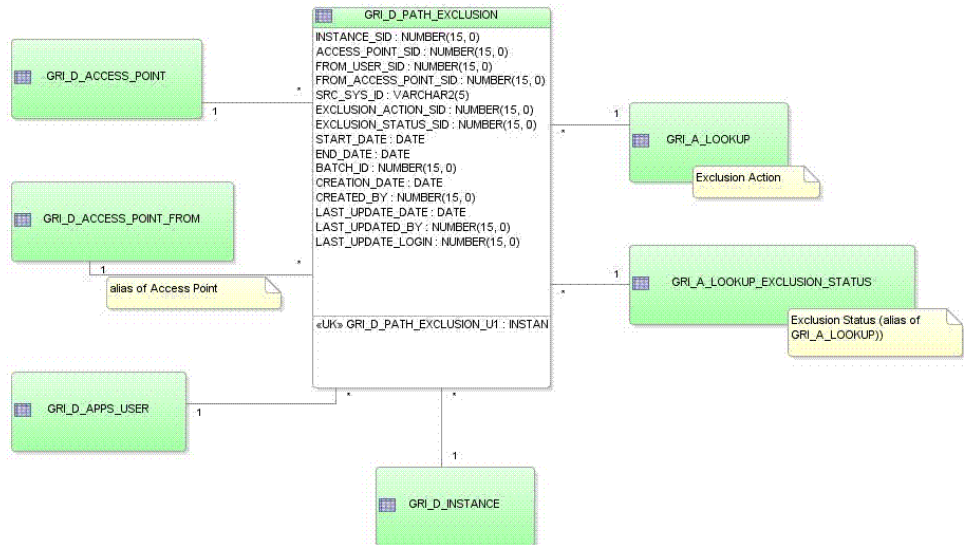
- Policy Detail Star



- Exclusions Star

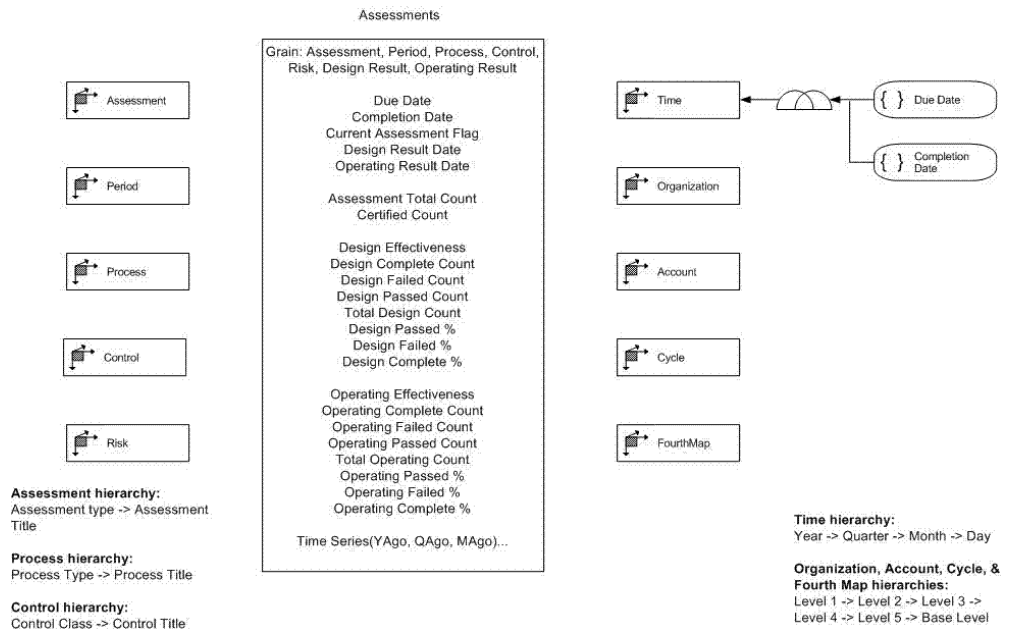


- Path Exclusions Star

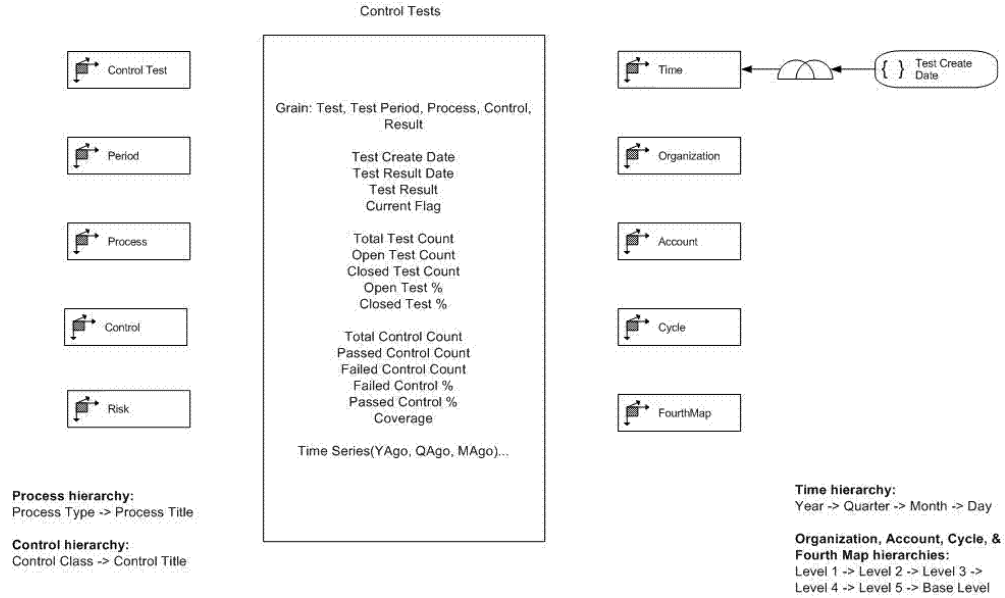


GRCI - GRCM 7.8 Logical Model

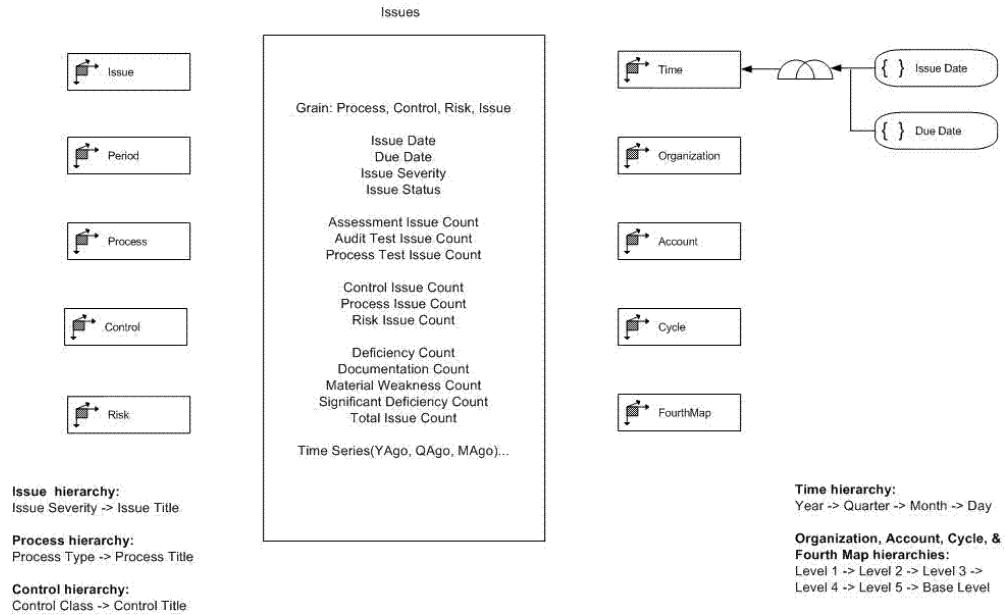
- Assessments



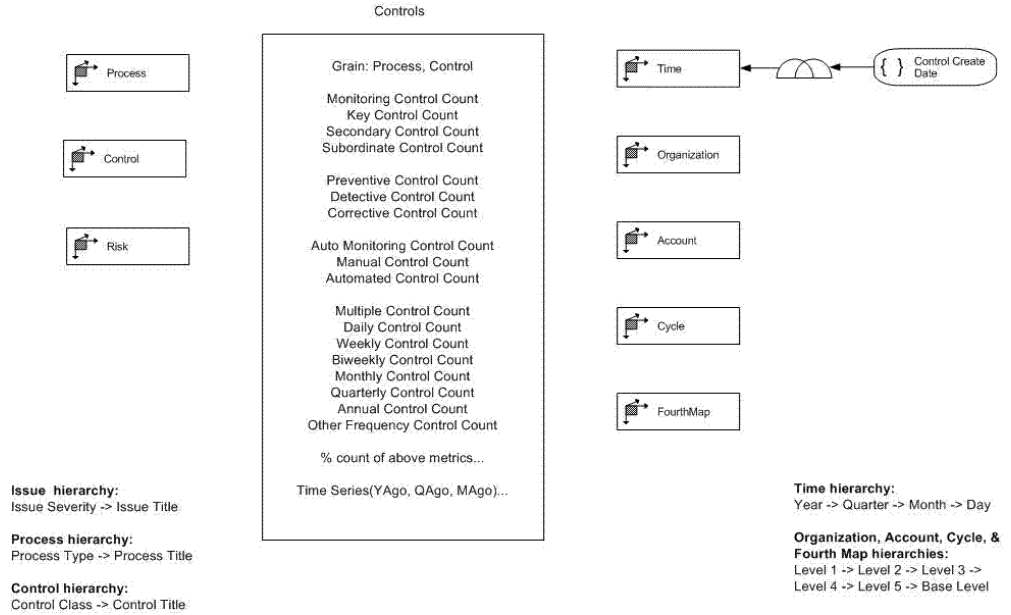
- Control Tests



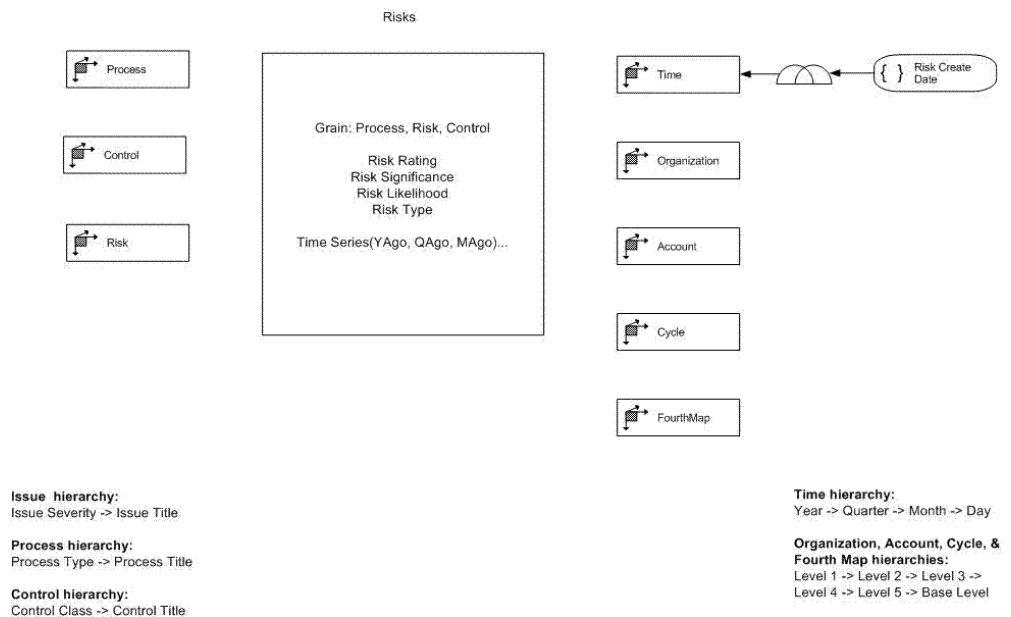
- Issues



- Controls

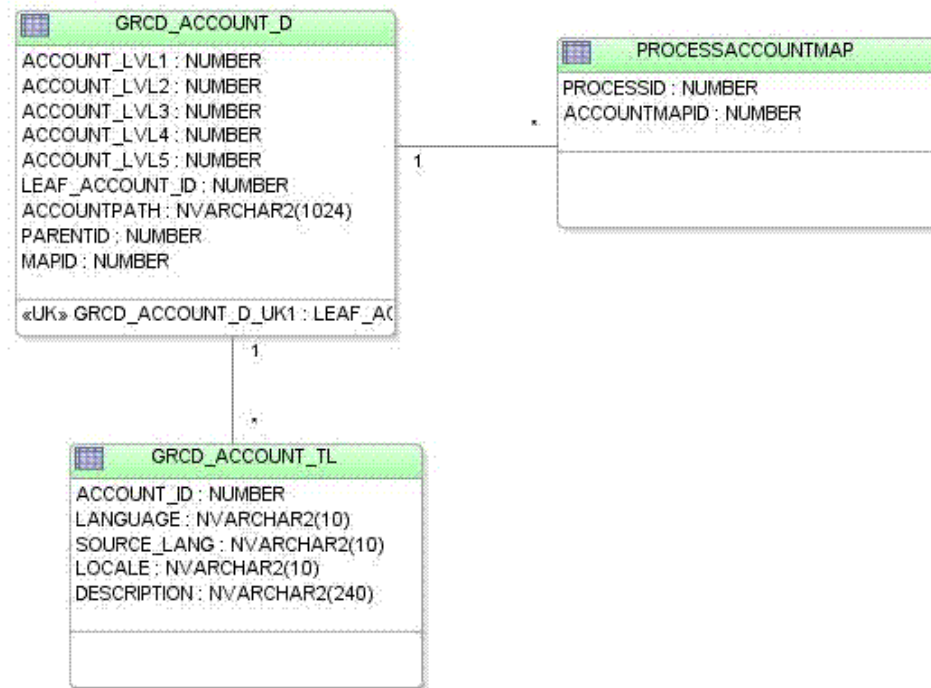


- Risks

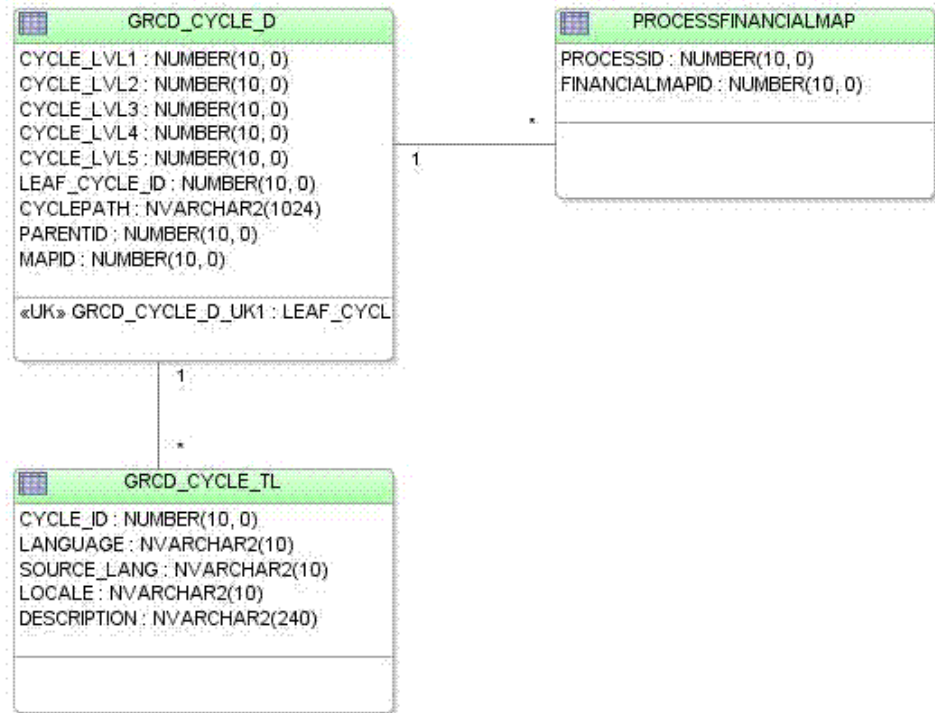


GRCI - GRM 7.8 Physical Model

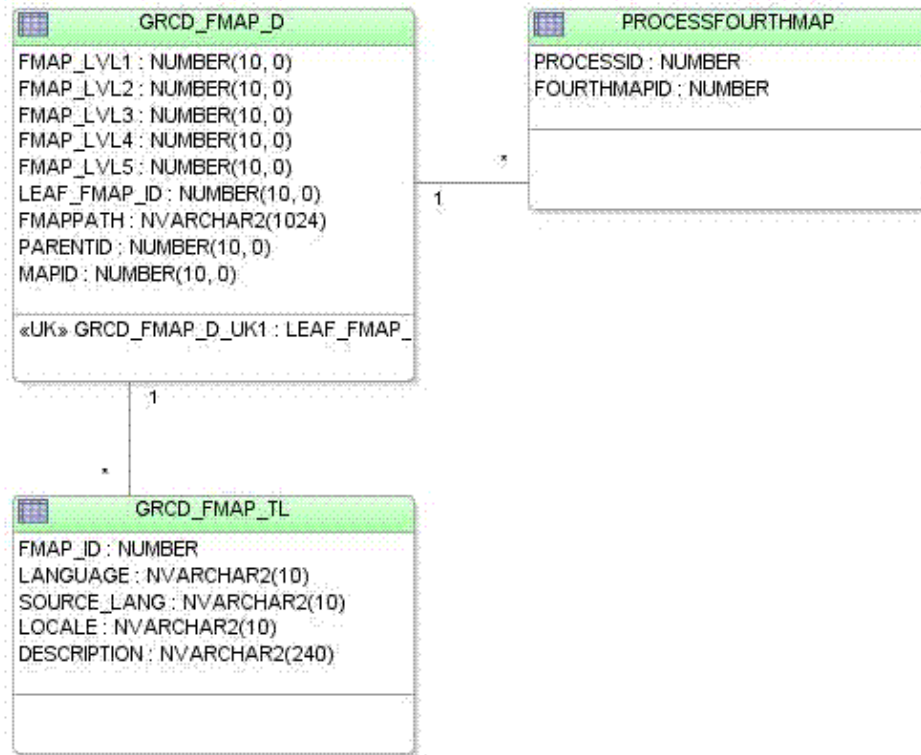
- Account



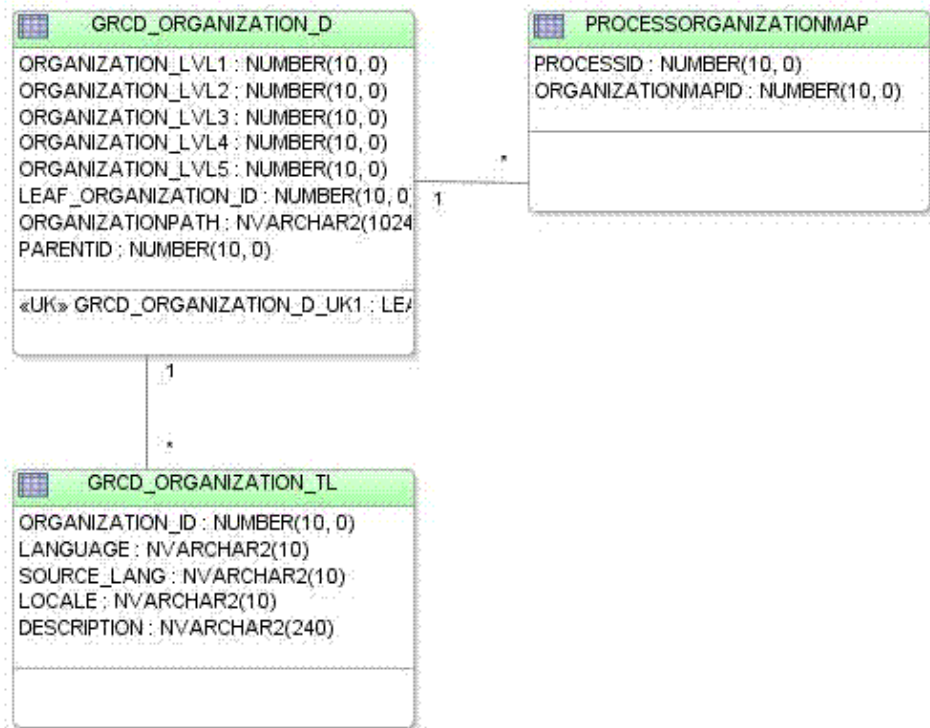
- Cycle



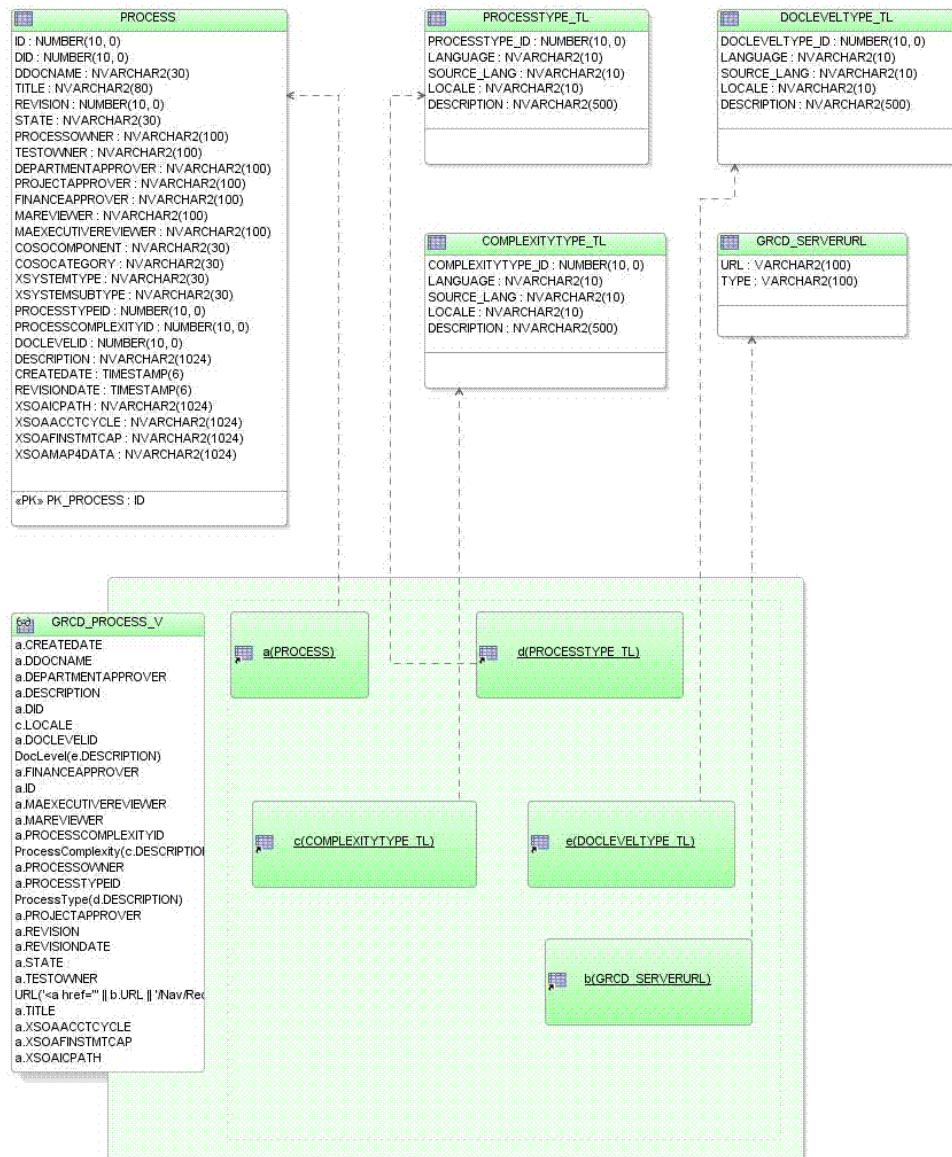
- Fourth Map



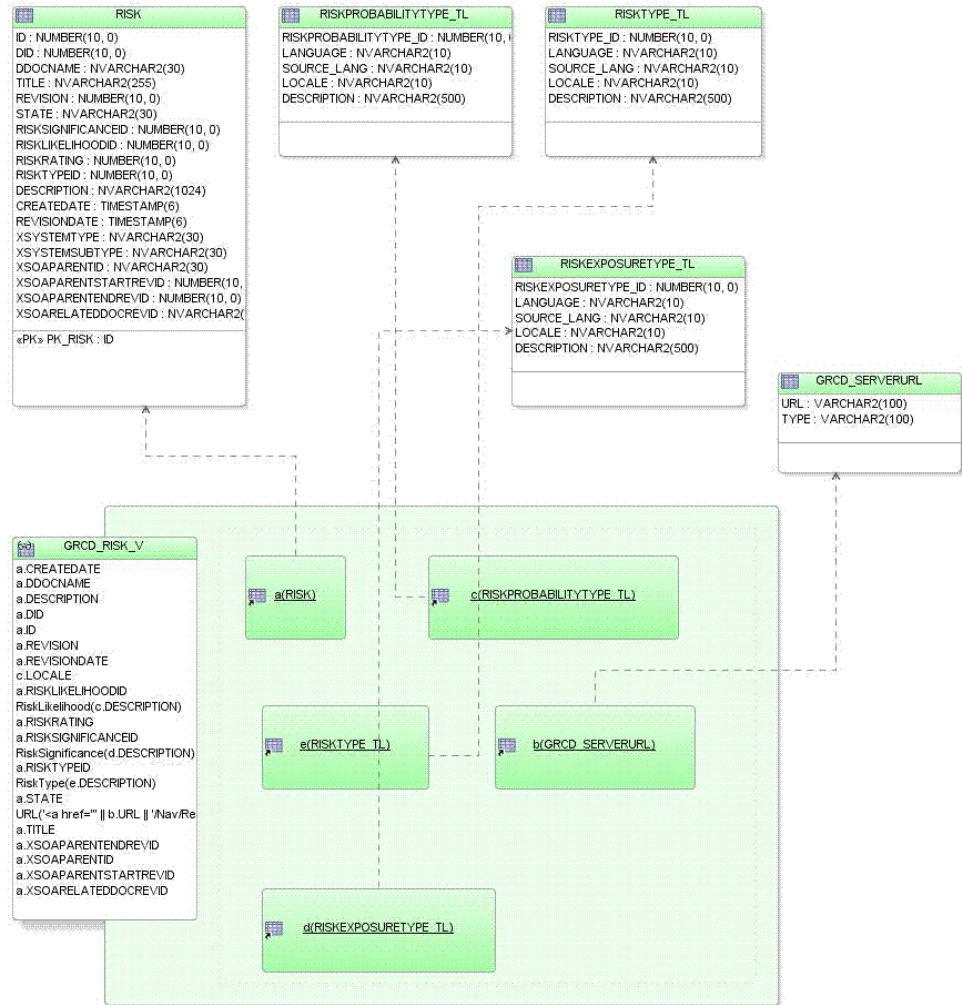
- Organization



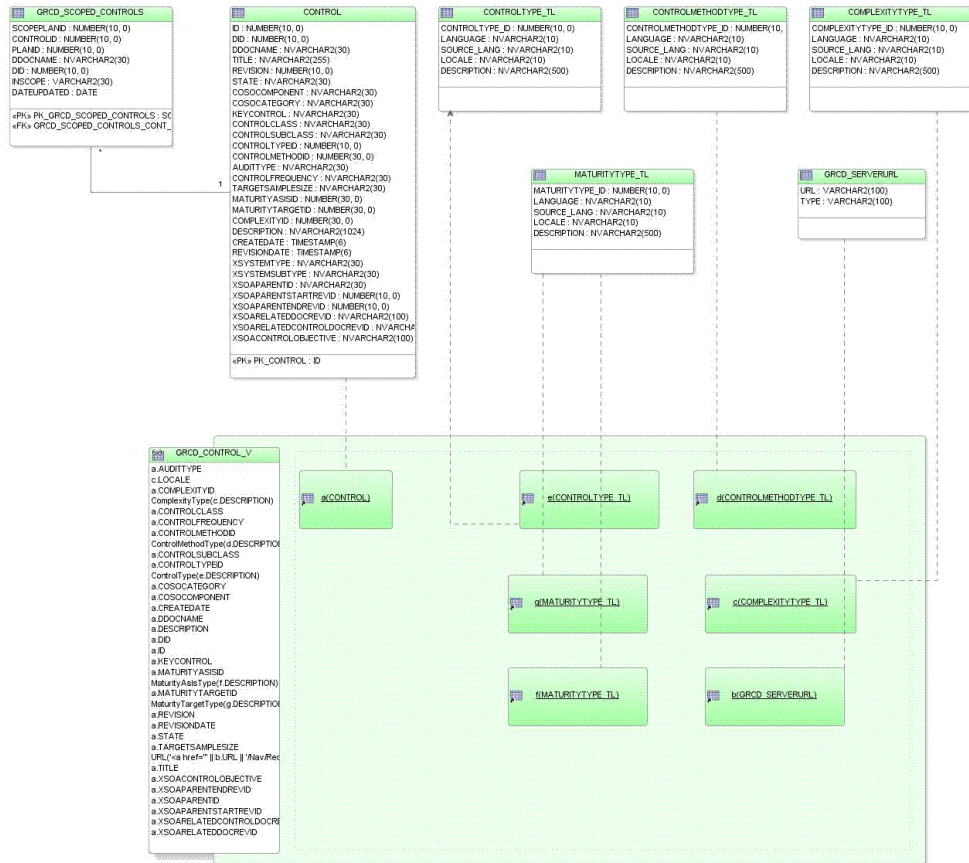
- Process



- Risk



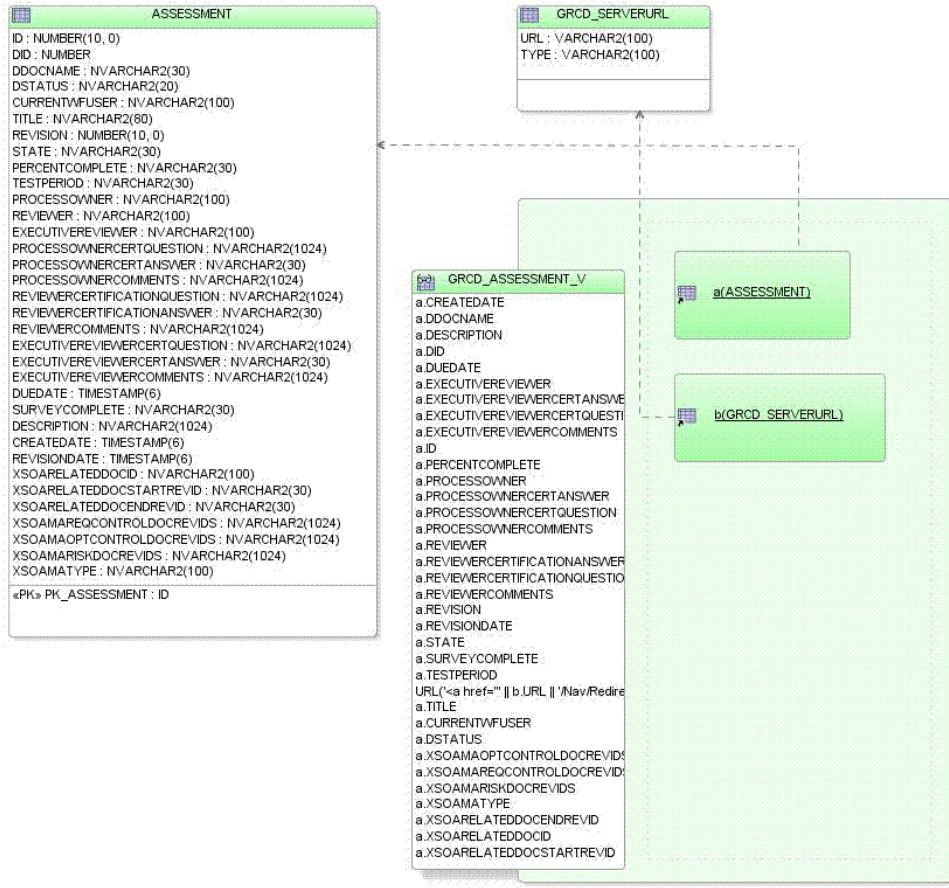
- Control



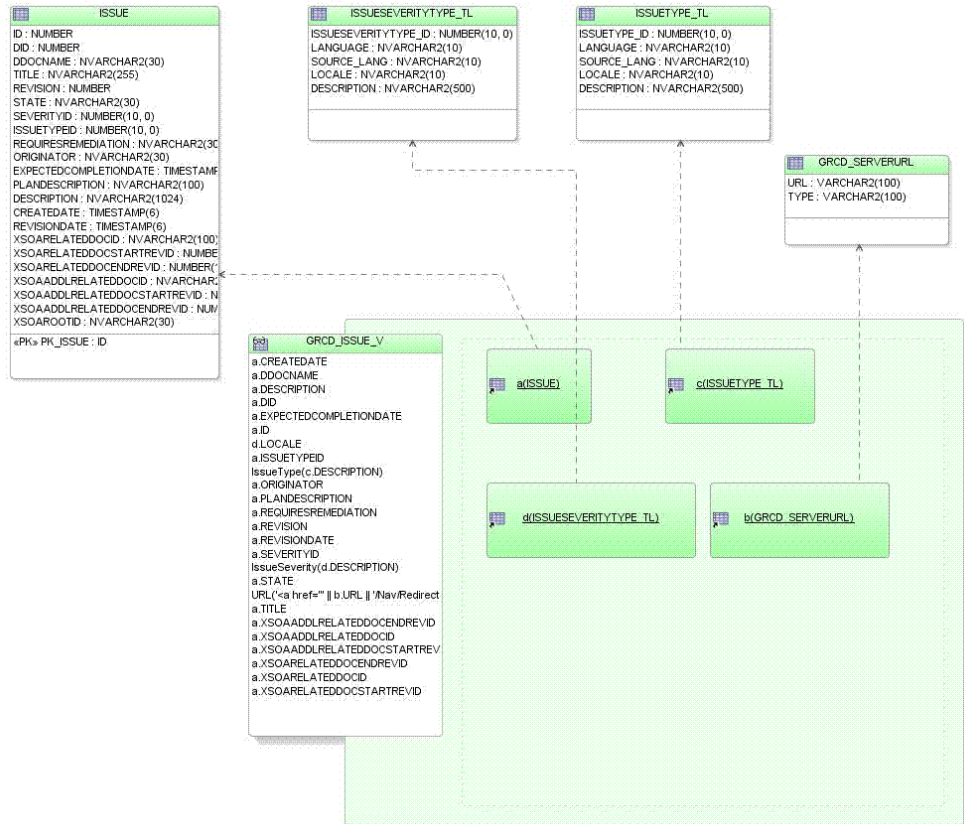
- Control Test



- Assessment



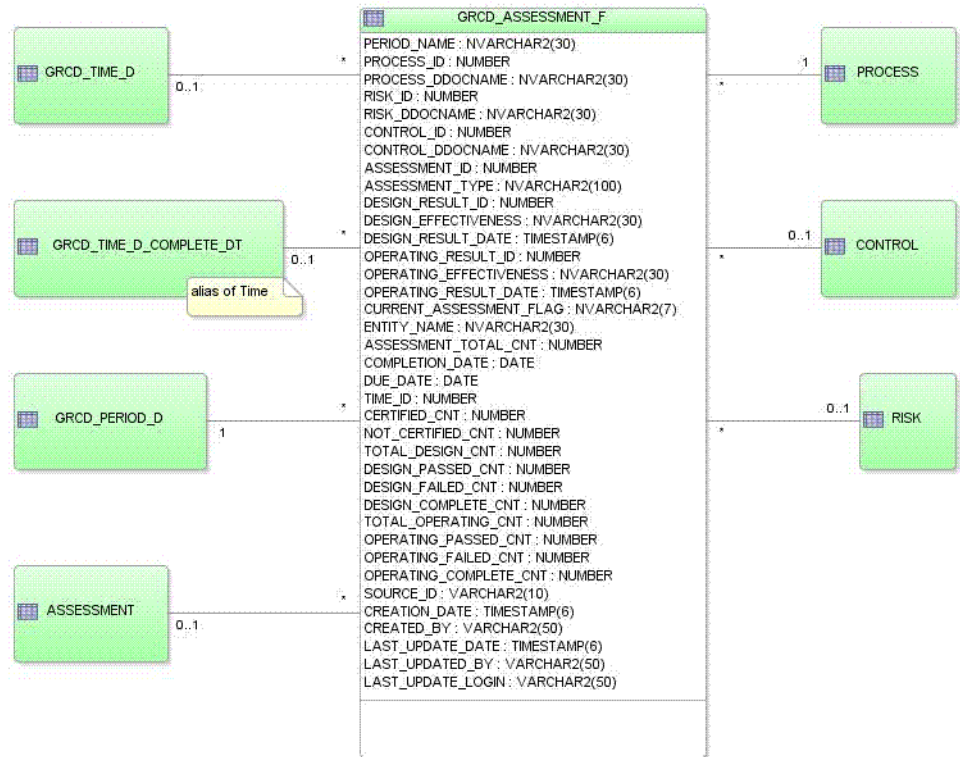
- Issue



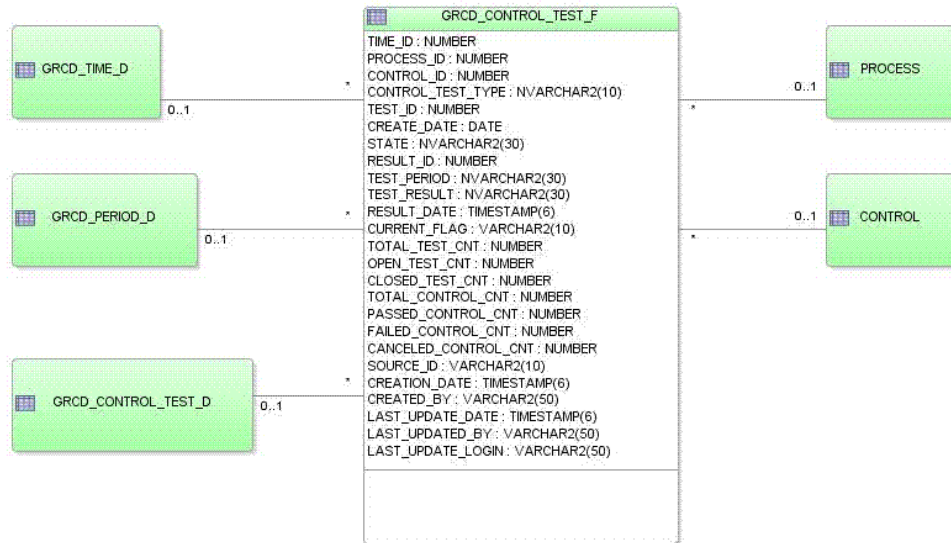
- Time



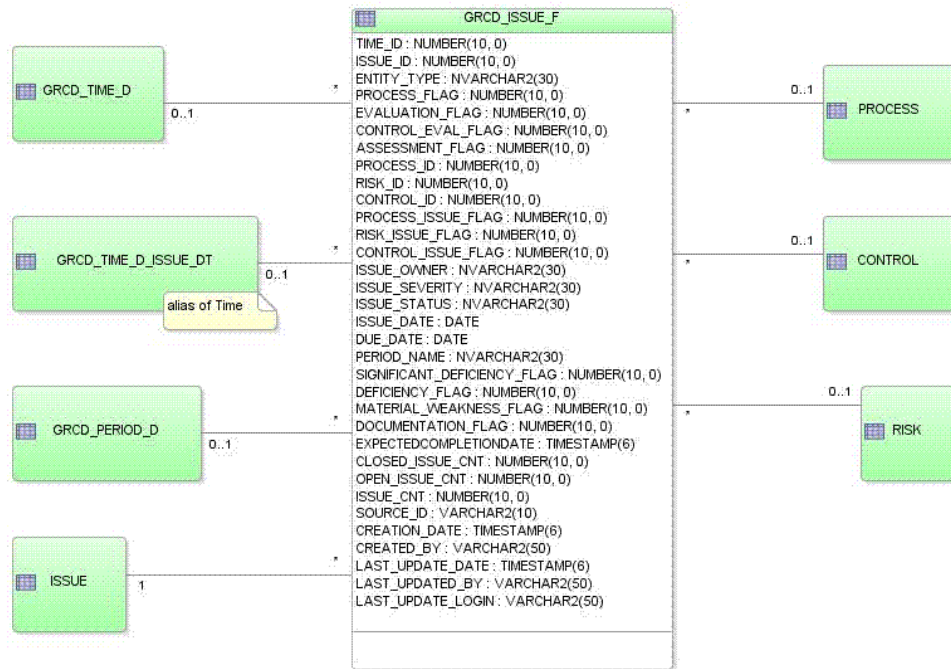
- Assessments Star



- Control Tests Star



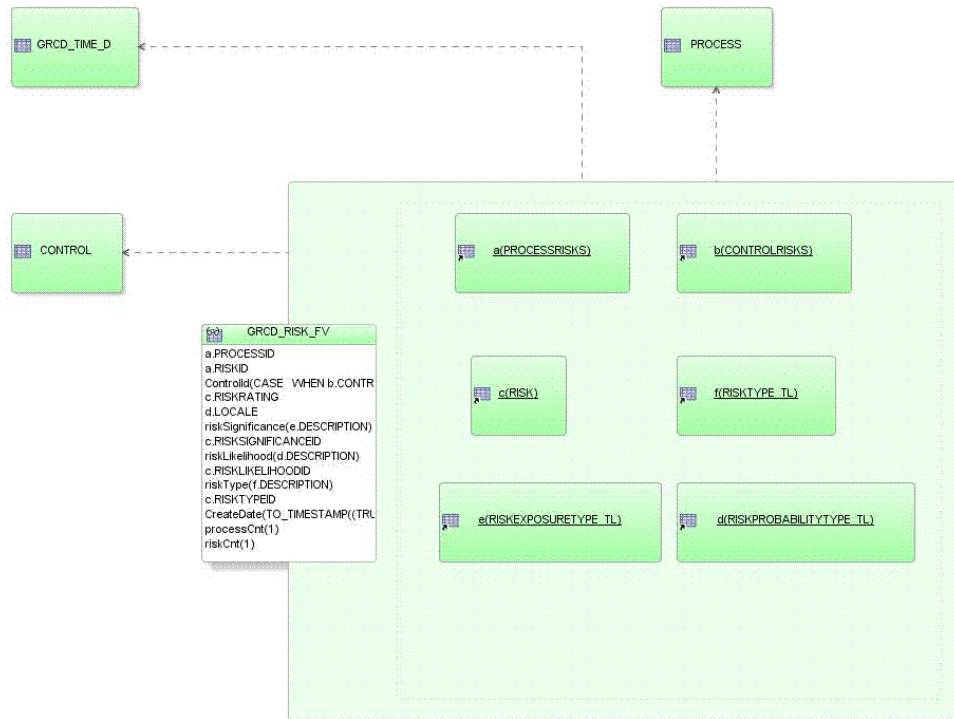
- Issues Star



- Controls Star



- Risks Star



Lineage for GRCM 7.8

This appendix covers the following topics:

- GRCI 2.0 - GRCM 7.8 Data Lineage CONSTANTS Table
- GRCI 2.0 - GRCM 7.8 Data Lineage DIMENSIONS Table
- GRCI 2.0 - GRCM 7.8 Data Lineage FACTS Table

GRCI 2.0 - GRCM 7.8 Data Lineage CONSTANTS Table

The following table provides lineage information on **constants**, such as type values, that are loaded from GRCM into GRCI.

Common Table Values

The following parameters have common values for all rows in this table.

- **Load Type:** Script
- **File Name:** Constants_Load_pkg.sql

Source Table Name	Constant Values	GRCI- Target Table Name	Create Procedure(s)	Load Procedure(s)
N/A	1 - 'Low'	COMPLEXITYTYPE	CREATECOMPLEXITYTYPE	LOADCOMPLEXITYTYPE
	2 - 'Med-Low'			
	3 - 'Medium'			
	4 - 'Med-High'			
	5 - 'High'			

Source Table Name	Constant Values	GRCI- Target Table Name	Create Procedure(s)	Load Procedure(s)
GRC_RESOURCE_STRINGS_TL ComplexityType	N/A	COMPLEXITYTYPE_TL		LOADCOMPLEXITYTYPE_TL
N/A	1 - 'Manual' 2 - 'Automated' 3 - 'Monitoring'	CONTROLMETHODTYPE	CREATECONTROLMETHODTYPE	LOADCONTROLMETHODTYPE
GRC_RESOURCE_STRINGS_TL ControlMethodType	N/A	CONTROLMETHODTYPE_TL		LOADCONTROLMETHODTYPE_TL
N/A	1 - 'Preventive' 2 - 'Detective' 3 - 'Corrective'	CONTROLTYPE	CREATECONTROLTYPE	LOADCONTROLTYPE
GRC_RESOURCE_STRINGS_TL ControlType	N/A	CONTROLTYPE_TL	CREATECONTROLTYPE	LOADCONTROLTYPE_TL
N/A	1 - 'Low' 2 - 'Med-Low' 3 - 'Medium' 4 - 'Med-High' 5 - 'High'	DOCLEVELTYPE	CREATEDOCLEVELTYPE	LOADDOCLEVELTYPE
GRC_RESOURCE_STRINGS_TL DocLevelType	N/A	DOCLEVELTYPE_TL	CREATEDOCLEVELTYPE	LOADDOCLEVELTYPE_TL

Source Table Name	Constant Values	GRCI- Target Table Name	Create Procedure(s)	Load Procedure(s)
N/A	http://localhost/ OracleGRCManager' 'http://localhost/ analytics/saw.dll ?Dashboard'	GRCD_SERVER URL	CREATESEVER RURL	LOADSERVERU RL
N/A	0 - 'Material Weakness' 1 - 'Significant Deficiency' 2 - 'Deficiency' 3 - 'Documentation Only'	ISSUESEVERITY TYPE	CREATEISSUES EVERITYTYPE	LOADISSUESEV ERITYTYPE
GRC_RESOURCE_STRINGS_TL IssueSeverityType	N/A	ISSUESEVERITY TYPE_TL	CREATEISSUES EVERITYTYPE	LOADISSUESEV ERITYTYPETL
N/A	0 - 'Process' 1 - 'Evaluation' 2 - 'Control Evaluation' 3 - 'Assessment'	ISSUETYPE	CREATEISSUET YPE	LOADISSUETYP E
GRC_RESOURCE_STRINGS_TL IssueType	N/A	ISSUETYPE_TL	CREATEISSUET YPE	LOADISSUETYP ETL

Source Table Name	Constant Values	GRCI- Target Table Name	Create Procedure(s)	Load Procedure(s)
N/A	1 - 'Unreliable' 2 - 'Informal' 3 - 'Standardized' 4 - 'Monitored' 5 - 'Optimized'	MATURITYTYPE	CREATEMATURITYTYPE	LOADMATURITYTYPE
GRC_RESOURCE_STRINGS_TL MaturityType	N/A	MATURITYTYPE_TL	CREATEMATURITYTYPE	LOADMATURITYTYPE_TL
N/A	1 - 'Process' 2 - 'Policy'	PROCESSTYPE	CREATEPROCESSTYPE	LOADPROCESSTYPE
GRC_RESOURCE_STRINGS_TL ProcessType	N/A	PROCESSTYPE_TL	CREATEPROCESSTYPE	LOADPROCESSTYPE_TL
N/A	1 - 'Low' 2 - 'Med-Low' 3 - 'Medium' 4 - 'Med-High' 5 - 'High'	RISKEXPOSURETYPE	CREATERISKEXPOSURETYPE	LOADRISKEXPOSURETYPE
GRC_RESOURCE_STRINGS_TL RiskExposureType	N/A	RISKEXPOSURETYPE_TL	CREATERISKEXPOSURETYPE	LOADRISKEXPOSURETYPE_TL

Source Table Name	Constant Values	GRCI- Target Table Name	Create Procedure(s)	Load Procedure(s)
N/A	1 - 'Negligible' 2 - 'Low' 3 - 'Medium' 4 - 'High' 5 - 'Extreme'	RISKPROBABILITYTYPE	CREATERISKPROBABILITYTYPE	LOADRISKPROBABILITYTYPE
GRC_RESOURCE_STRINGS_TL RiskProbabilityType	N/A	RISKPROBABILITYTYPE_TL	CREATERISKPROBABILITYTYPE	LOADRISKPROBABILITYTYPE_TL
N/A	1 - 'Financial Fraud' 2 - 'Theft of Assets' 3 - 'Theft of Services' 4 - 'Regulatory Compliance' 5 - 'Breach of Security'	RISKTYPE	CREATERISKTYPE	LOADRISKTYPE
GRC_RESOURCE_STRINGS_TL RiskType	N/A	RISKTYPE_TL	CREATERISKTYPE	LOADRISKTYPE_ETL

GRCI 2.0 - GRM 7.8 Data Lineage DIMENSIONS Table

The following tables contain the GRM source table name that loads the GRCI **dimensions**, the procedure name that performs the load, and the file that contains the procedure.

Common Table Values

The following parameters have common values for all rows in this table.

- **Load Type:**Script

- **File Name:** Dims_Load_pkg.sql (*except where noted.*)

Source Table Name	GRCI - Target Table Name	Create Procedure(s)	Load Procedure(s)
1. PROCESS	ACCOUNTMAP	CREATEACCOUNTMAP	LOADACCOUNTMAP
2. GRCD_ACCOUNT_D			
vwDocumentHistory	ASSERTION	CREATEASSERTION	LOADASSERTION
1. vwDocumentHistory	ASSESSMENT	CREATEASSESSMENT	LOADASSESSMENT
2. Default Dimension Values			
vwDocumentHistory	AUDITTEST	CREATEAUDITTEST	LOADAUDITTEST
1. AuditTest	AUDITTESTCONTROLS	CREATEAUDITTESTCONTROLS	LOADAUDITTESTCONTROLS
2. Control			
1. vwDocumentHistory	CONTROL	CREATECONTROL	LOADCONTROL
2. ControlType			
3. ControlMethodType			
4. MaturityAsIsType			
5. MaturityTargetType			
6. ComplexityType			

Source Table Name	GRCI - Target Table Name	Create Procedure(s)	Load Procedure(s)
1. Control	CONTROLRISKS	CREATECONTROLRISKS	LOADCONTROLRISKS
2. Risk			
1. Process	FINANCIALMAP	CREATEFINANCIALMAP	LOADFINANCIALMAP
2. GRCD_CYCLE_D			
PROCESS	FOURTHMAP	CREATEFOURTHMAP	LOADFOURTHMAP
1. GRC_MAP_NO DES	GRCD_ACCOUNT_D	CREATEACCOUNTD	LOADACCOUNTD
2. GRC_MAPS			
1. GRC_MAP_NO DES_TL	GRCD_ACCOUNT_TL	CREATEACCOUNTTL	LOADACCOUNTTL
2. GRC_MAPS			
CONTROL	GRCD_CONTROL_HIERARCHY_B	CREATECONTROLHIERARCHYB	LOADCONTROLHIERARCHYB
Default Dimension Values	GRCD_CONTROL_TEST_D	CREATECONTROLTESTD	LOADCONTROLTESTD
GRC_MAPS, GRC_MAP_NODES	GRCD_CYCLE_D	CREATECYCLED	LOADCYCLED
GRC_MAPS, GRC_MAP_NODES_TL	GRCD_CYCLE_TL	CREATECYCLETL	LOADCYCLETL
GRC_MAPS, GRC_MAP_NODES	GRCD_FMAP_D	CREATEFMAPD	LOADFMAPD

Source Table Name	GRCI - Target Table Name	Create Procedure(s)	Load Procedure(s)
GRC_MAPS, GRC_MAP_NODES_ TL	GRCD_FMAP_TL	CREATEFMAPTL	LOADFMAPTL
GRC_MAPS, GRC_MAP_NODES	GRCD_ORGANIZATI ON_D	CREATEORGANIZA TIOND	LOADORGANIZATI OND
GRC_MAPS, GRC_MAP_NODES_ TL	GRCD_ORGANIZATI ON_TL	CREATEORGANIZA TIONTL	LOADORGANIZATI ONTL
GRC_FISCAL_PERIO DS	GRCD_PERIOD_D	CREATETIMED	LOADTIMED
GRC_FISCAL_PERIO DS	GRCD_TIME_D	CREATE_GRCD_TIM E_D	LOAD_GRCD_TIME _D
File Name: Execute_Load_GRCD _TIME_D.sql			
UserSecurityAttribute s	GRCD_USER_ROLE	CREATEUSERROLE	LOADUSERROLE
UserSecurityAttribute s	GRCD_USERS	CREATEUSERS	LOADUSERS
vwDocumentHistory DocMeta, Revisions, Documents	ISSUE	CREATEISSUE	LOADISSUE
PROCESS ORGANIZATIONM AP, GRCD_ORGANIZAT ION_D	ORGANIZATIONM AP	CREATEORGANIZA TIONMAP	LOADORGANIZATI ONMAP

Source Table Name	GRCI - Target Table Name	Create Procedure(s)	Load Procedure(s)
VwDocumentHistory ProcessType, ComplexityType, DocLevelType	PROCESS	CREATEPROCESS	LOADPROCESS
PROCESS ACCOUNTMAP	PROCESSACCOUNT MAP	CREATEPROCESSA CCOUNTMAP	LOADPROCESSACC OUNTMAP
Assessment Process	PROCESSASSESSME NTS	CREATEPROCESSAS SESSMENTS	LOADPROCESSASSE SSMENTS
Control Process	PROCESSCONTROL S	CREATEPROCESSC ONTROLS	LOADPROCESSCON TROLS
Process, FinancialMap	PROCESSFINANCIA LMAP	CREATEPROCESSFI NANCIALMAP	LOADPROCESSFIN ANCIALMAP
Process, FourthMap	PROCESSFOURTHM AP	CREATEPROCESSFO URTHMAP	LOADPROCESSFOU RTHMAP
Process p OrganizationMap o	PROCESSORGANIZ ATIONMAP	CREATEPROCESSO RGANIZATIONMAP	LOADPROCESSORG ANIZATIONMAP
Risk, Process	PROCESSRISKS	CREATEPROCESSRI SKS	LOADPROCESSRISK S
vwDocumentHistory	PROCESSTEST	CREATEPROCESSTE ST	LOADPROCESSTEST

Source Table Name	GRCI - Target Table Name	Create Procedure(s)	Load Procedure(s)
vwDocumentHistory, RiskExposureType, RiskProbabilityType RiskType, Default Dimensionvalues	RISK	CREATERISK	LOADRISK
GRC_SCOPED_CON TROLS, CONTROL	GRCD_SCOPED_CO NTROLS		LOADSCOPEDCON TROLS
GRC_SCOPE_PLANS	GRCD_SCOPE_PLA NS		LOADSCOPEPLANS

GRCI 2.0 - GRM 7.8 Data Lineage FACTS Table

The following tables contain the GRM source table name that loads the GRCI **facts**, the procedure that performs the load, and the file that contains the procedure.

Common Table Values

The following parameters have common values for all rows in this table.

- **Load Type:** Script
- **File Name:** Facts_Load_pkg.sql

Source Table Name	GRCI - Target Table Name	Create Procedure(s)	Load Procedure(s)
1. ControlDesignRe sult	ASSESSMENTCONT ROLDDESIGNRESULT S	CREATEASSESSCTC DESIGNRESULTS	LOADASSESSCONT ROLDDESIGNRESULT S
2. ASSESSMENT			

Source Table Name	GRCI - Target Table Name	Create Procedure(s)	Load Procedure(s)
1. ControlOperatingResult	ASSESSMENTCONTROLOPRESULTS	CREATEASSESSCONTROLOPRESULTS	LOADASSESSMENTCONTROLOPRESULTS
2. ASSESSMENT			
1. ProcessDesignResult	ASSESSMENTPROCESSDESIGNRESULTS	CREATEASSESSBPCDESIGNRESULTS	LOADASSESSPROCESSDESIGNRESULTS
2. Assessment			
1. ProcessOperatingResult	ASSESSMENTPROCESSOPRESULTS	CREATEASSESSPROCESSOPRESULTS	LOADASSESSMENTPROCESSOPRESULTS
2. Assessment			
1. RiskDesignResult	ASSESSMENTRISKDESIGNRESULTS	CREATEASSESSRISKDESIGNRESULTS	LOADASSESSRISKDESIGNRESULTS
2. Assessment			
1. RiskOperatingResult	ASSESSMENTRISKOPERATINGRESULTS	CREATEASSESSMENTRISKOPRESULTS	LOADASSESSMENTRISKOPRESULTS
2. Assessment			
1. vwDocumentHistory	AUDITTESTRESULT	CREATEAUDITTESTRESULT	LOADAUDITTESTRESULT
2. Control			
1. AuditTestResult	AUDITTESTRESULTS	CREATEAUDITTESTRESULTS	LOADAUDITTESTRESULTS
2. AuditTest			
vwDocumentHistory, Control	CONTROLDESIGNRESULT	CREATECONTROLDESIGNRESULT	LOADCONTROLDESIGNRESULT

Source Table Name	GRCI - Target Table Name	Create Procedure(s)	Load Procedure(s)
VwDocumentHistory, Control	CONTROLOPERATINGRESULT	CREATECONTROLOPERATINGRESULT	LOADCONTROLOPERATINGRESULT

Source Table Name		GRCI - Target Table Name	Create Procedure(s)	Load Procedure(s)
1.	PROCESS	GRCD_ASSESSMENT_F	CREATEASSESSMENTF	LOADASSESSMENTF
2.	PROCESSCONTROLS			
3.	CONTROL			
4.	ASSESSMENT			
5.	ASSESSMENTCONTROLDESIGNRESULTS			
6.	CONTROLDESIGNRESULT			
7.	AssessmentControlOpResults			
8.	CONTROLOPERATINGRESULT			
9.	ProcessRisks			
10.	AssessmentRiskDesignResults			
11.	RiskDesignResult			
12.	ASSESSMENTRISKOPERATINGRESULTS			
13.	RISKOPERATINGRESULT			
14.	PROCESSASSESSMENTS			
15.	ASSESSMENTPROCESSDESIGNRESULTS			

Source Table Name	GRCI - Target Table Name	Create Procedure(s)	Load Procedure(s)
16. PROCESSDESIGNRESULT			
17. AssessmentProcessOpResults			
18. PROCESSOPERATINGRESULT			
1. AuditTest	GRCD_AUDIT_TEST_RESULT_F	CREATEAUDITTESTRESULTF	LOADAUDITTESTRESULTF
2. AuditTestResults			
3. AuditTestResult			
4. AuditTestControls			
5. Control			
6. ProcessControls			
7. Process			
1. GRCD_PROCESSTEST_RESULT_F	GRCD_CONTROL_TEST_F	CREATECONTROLTESTF	LOADCONTROLTESTF
2. ProcessTest			
3. GRCD_AUDIT_TEST_RESULT_F			
4. AuditTest			
Issue Risk Control	GRCD_ISSUE_F	CREATEISSUEF	LOADISSUEF

Source Table Name	GRCI - Target Table Name	Create Procedure(s)	Load Procedure(s)
Process ProcessTest ProcessTestResult ProcessTestResults	GRCD_PROCESS_TEST_RESULT_F	CREATEPROCESSTESTRESULTF	LOADPROCESSTESTRESULTF
VwDocumentHistory Process	PROCESSDESIGNRESULT	CREATEPROCESSDESIGNRESULT	LOADPROCESSDESIGNRESULT
VwDocumentHistory Process	PROCESSOPERATINGRESULT	CREATEPROCESSOPERATINGRESULT	LOADPROCESSOPERATINGRESULT
VwDocumentHistory Control	PROCESSTESTRESULT	CREATEPROCESSTESTRESULT	LOADPROCESSTESTRESULT
ProcessTestResult	PROCESSTESTRESULTS	CREATEPROCESSTESTRESULTS	LOADPROCESSTESTRESULTS
VwDocumentHistory Risk	RISKDESIGNRESULT	CREATERISKDESIGNRESULT	LOADRISKDESIGNRESULT
VwDocumentHistory Risk	RISKOPERATINGRESULT	CREATERISKOPERATINGRESULT	LOADRISKOPERATINGRESULT

Lineage for AACG 8.1.1 or Later

This appendix covers the following topics:

- GRCI 2.0 - AACG 8.1.1 or Later, Data Lineage DIMENSIONS Table
- GRCI 2.0 - AACG 8.1.1 or Later, Data Lineage FACTS Table

GRCI 2.0 - AACG 8.1.1 or Later, Data Lineage DIMENSIONS Table

The following table contains the GRCI staging table name that loads the GRCI **dimensions**, and the package that loads the target GRCI dimension table.

It is important to note that all these packages are invoked from GRI_MASTER_PKG

Common Table Values

The following parameters have common values for all rows in this table.

- **Master Package:** GRI_MASTER_PKG

Error Table Name	Dimension/Bridge Table Package	Create Procedure(s)	Package Name	Sub-Package Name	Interface Name
	GRI_DIMENSIONS_PKG		GRI_INSTANCE_PKG	GRI_D_INSTANCE_PKG	GRI_D_INSTANCE_INTR
	GRI_DIMENSIONS_PKG		GRI_INSTANCE_PKG	GRI_D_INSTANCE_TL_PKG	GRI_D_INSTANCE_TL_INTR
	GRI_DIMENSIONS_PKG		GRI_GENERIC_DIM_PKG	GRI_D_GENERIC_DIM_PKG	GRI_D_GENERIC_DIM_INTR

Error Table Name	Dimension/Bridge Table Package	Create Procedure(s)	Package Name	Sub-Package Name	Interface Name
	GRI_DIMENSIONS_PKG		GRI_GENERIC_DIM_PKG	GRI_D_GENERIC_DIM_TL_PKG	GRI_D_GENERIC_DIM_TL_INTR
GRI_E_GENERIC_DIM_VAL	GRI_DIMENSIONS_PKG		GRI_GENERIC_DIM_PKG	GRI_D_GENERIC_DIM_VAL_PKG	GRI_D_GENERIC_DIM_VAL_INTR
	GRI_DIMENSIONS_PKG		GRI_GENERIC_DIM_PKG	GRI_D_GENERIC_DIM_VAL_TL_PKG	GRI_D_GENERIC_DIM_VAL_TL_INTR
	GRI_DIMENSIONS_PKG	CREATEACCOUNTMAP	GRCD_USER_MAIN_PKG	GRCD_USER_PKG	GRCD_USER_INTR
	GRI_DIMENSIONS_PKG		GRCD_USER_MAIN_PKG	GRCD_USER_TL_PKG	GRCD_USER_TL_INTR
GR_E_POLICY	GRI_DIMENSIONS_PKG		GRI_POLICY_PKG	GRI_D_POLICY_PKG	GRI_D_POLICY_INTR
	GRI_DIMENSIONS_PKG		GRI_POLICY_PKG	GRI_D_POLICY_TL_PKG	GRI_D_POLICY_TL_INTR
GRI_E_ENTITLEMENT	GRI_DIMENSIONS_PKG		GRI_ENTITLEMENT_PKG	GRI_D_ENTITLEMENT_PKG	GRI_D_ENTITLEMENT_INTR
	GRI_DIMENSIONS_PKG	CREATEASSERTION	GRI_ENTITLEMENT_PKG	GRI_D_ENTITLEMENT_TL_PKG	GRI_D_ENTITLEMENT_TL_INTR
	GRI_DIMENSIONS_PKG	CREATEASSESSMENT	GRI_ACCESS_POINT_PKG	GRI_D_ACCESS_POINT_PKG	GRI_D_ACCESS_POINT_INTR
	GRI_DIMENSIONS_PKG	CREATEAUDITTEST	GRI_ACCESS_POINT_PKG	GRI_D_ACCESS_POINT_TL_PKG	GRI_D_ACCESS_POINT_TL_INTR

Error Table Name	Dimension/Bridge Table Package	Create Procedure(s)	Package Name	Sub-Package Name	Interface Name
	GRI_DIMENSIONS_PKG	CREATEAUDITTESTCONTROLS	GRI_APPS_USER_PKG	GRI_D_APPS_USER_PKG	GRI_D_APPS_USER_INTR
	GRI_DIMENSIONS_PKG	CREATECONTROL	GRI_APPS_USER_PKG	GRI_D_APPS_USER_TL_PKG	GRI_D_APPS_USER_TL_INTR
	GRI_DIMENSIONS_PKG	CREATECONTROLRISKS	GRI_ROLE_PKG	GRI_D_ROLE_PKG	GRI_D_ROLE_INTR
	GRI_DIMENSIONS_PKG	CREATEFINANCIALMAP	GRI_ROLE_PKG	GRI_D_ROLE_TL_PKG	GRI_D_ROLE_TL_INTR
	GRI_DIMENSIONS_PKG	CREATEFOURTHMAP	GRI_D_RUN_PKG	GRI_D_RUN_PKG	GRI_D_RUN_INTR
GRI_E_EXCLUSION	GRI_DIMENSIONS_PKG	CREATEACCOUNT	GRI_EXCLUSION_PKG	GRI_D_EXCLUSION_PKG	GRI_D_EXCLUSION_INTR
GRI_E_EXCLUSION_DETAIL	GRI_DIMENSIONS_PKG	CREATEACCOUNTTTL	GRI_EXCLUSION_PKG	GRI_D_EXCLUSION_DETAIL_PKG	GRI_D_EXCLUSION_DETAIL_INTR
GRI_E_PATH_EXCLUSION	GRI_DIMENSIONS_PKG	CREATECONTROLDIRECTORY	GRI_EXCLUSION_PKG	GRI_D_PATH_EXCLUSION_PKG	GRI_D_PATH_EXCLUSION_INTR
	GRI_BRIDGE_TABLES_PKG	CREATECONTROLTST	GRI_D_ROLE_USER_BG_PKG	GRI_D_ROLE_USER_BG_PKG	GRI_D_ROLE_USER_BG_INTR
	GRI_BRIDGE_TABLES_PKG	CREATECYCLED	GRI_D_POLICY_GENERAL_DIM_BG_PKG	GRI_D_POLICY_GENERAL_DIM_BG_PKG	GRI_D_POLICY_GENERAL_DIM_BG_INTR

Error Table Name	Dimension/Bridge Table Package	Create Procedure(s)	Package Name	Sub-Package Name	Interface Name
	GRI_BRIDGE_TABLES_PKG	CREATECYC LETL	GRI_D_POLI CY_DETAIL_ BG_PKG	GRI_D_POLI CY_DETAIL_ BG_PKG	GRI_D_POLI CY_DETAIL_ BG_INTR
	GRI_BRIDGE_TABLES_PKG	CREATEFM APD	GRI_D_ENTL MNT_GENE RIC_DIM_BG _PKG	GRI_D_ENTL MNT_GENE RIC_DIM_BG _PKG	GRI_D_ENTL MNT_GENE RIC_DIM_BG _INTR
	GRI_BRIDGE_TABLES_PKG	CREATEFM APTL	GRI_D_ENTI TLEMENT_A P_BG_PKG	GRI_D_ENTI TLEMENT_A P_BG_PKG	GRI_D_ENTI TLEMENT_A P_BG_INTR

GRCI 2.0 - AACG 8.1.1 or Later, Data Lineage FACTS Table

The following table contains the GRCI staging table name that loads the GRCI **fact** tables, and the package that loads the target GRCI fact table.

NOTE:It is important to note that all these packages are invoked from the fact package GRI_FACTS_PKG, which in turn is invoked from GRI_MASTER_PKG.

Common Table Values

The following parameters have common values for all rows in this table.

- **Load Type:**ODI
- **Master Package:**GRI_MASTER_PKG
- **Fact Package:**GRI_FACTS_PKG

SI NO.	Source Table Name(s)	Target Table Name	Error Table Name	Package Name	Interface Name
1	GRI_S_CONFLICTS GRI_D_RUN GRI_D_POLICY GRI_D_GBL_USER GRI_A_LOOKUP	GRI_F_CONFLICTS_T	GRI_E_CONFLICTS_T	GRI_F_CONFLICTS_T_PKG	GRI_F_CONFLICTS_T_INTR
2	GRI_F_CONFLICTS_T GRI_D_POLICY	GRI_D_POLICY_PREV_R UN_BG		GRI_D_POLICY_PREV_R UN_BG_PKG	GRI_D_POLICY_PREV_R UN_BG_INTR
3	GRI_S_CONFLICT_PATH GRI_D_RUN GRI_D_POLICY GRI_D_APPS_USER GRI_D_ACCESS_POINT GRI_D_ELEMENT GRCD_USERS GRI_A_LOOKUP	GRI_F_CONFLICT_PATH_T	GRI_E_CONFLICT_PATH_T	GRI_F_CONFLICT_PATH_T_PKG	GRI_F_CONFLICT_PATH_T_INTR

SI NO.	Source Table Name(s)	Target Table Name	Error Table Name	Package Name	Interface Name
4	GRI_S_CONF LICT_PATH GRI_D_RUN GRI_D_POLI CY GRI_D_POLI CY_INSTAN CE_V	GRI_F_CONF LICT_PATH_ T	GRI_E_CON FLICT_PATH _T	GRI_F_CONF LICT_PATH_ T_PKG_2	GRI_F_CONF LICT_PATH_ T_INTR_2

Index

A

AACG Logical Model, C-1

B

BI Publisher
Install reports, 2-24

C

Constants
GRCM, D-1
Creating the Target
Physical Model, 2-17

D

Data Flow
Diagram, B-1
Detailed Data, B-3
Dimensions, D-5
Dimensions Data Lineage
AACG, E-1

E

ETL Execution, A-2
ETL Execution Sequence
Sequence, A-1

F

Facts, D-10
Facts AACG, E-4

G

Governance, Risk and Compliance Intelligence
install, 1-3
overview, 1-1
GRCI - AACG 8.1.1 Physical Model, C-5
GRCM 7.8 and AACG 8.1.1, 4-1
GRCM Logical Model, C-19
GRCM Physical Model, C-21

I

Install, 1-4
Oracle Scripts, 2-1
Installation
Scripts, 3-1

L

Languages
GRCM, 1-3
Loading
Target Tables, 2-17

M

Multi-language
OBIEE, 2-19

O

OBIEE
Reports, 2-18
ODI Code
Install, 3-2

Overview, 2-1

P

Package, A-3

S

Security Integration

AACG, 3-13

Optional, 2-28

Set Up

Environment, 2-2

U

Upgrading, 4-2