Oracle® Enterprise Governance, Risk and Compliance

Implementation Guide

Release 8.0.1

Part No. E17454-01

March 2010

ORACLE

Oracle Enterprise Governance, Risk and Compliance Implementation Guide, Release 8.0.1

Part No. E17454-01

Primary Author: Denise Fairbanks Simpson

Contents

Send Us Your Comments

Oracle Enterprise Governance, Risk and Compliance Implementation Guide, Release 8.0.1

Part No. E17454-01

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

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

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

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

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

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

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

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

Preface

Intended Audience

Welcome to Release 8.0.1 of the *Oracle Enterprise Governance, Risk and Compliance Implementation Guide.*

This guide is intended for information technology personnel and privileged users who are responsible for installing and configuring the Oracle Enterprise Governance, Risk and Compliance Manager (EGRCM) application. It assumes the reader is familiar with Oracle Application Server 11gR1 installation, configuration, and use.

See Related Information Sources on page viii for more Oracle E-Business Suite product information.

Deaf/Hard of Hearing Access to Oracle Support Services

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

Documentation Accessibility

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

For more information, visit the Oracle Accessibility Program Web site at http://www.oracle.com/accessibility/.

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

Structure

Related Information Sources

Oracle Enterprise Governance, Risk and Compliance Manager User's Guide

Do Not Use Database Tools to Modify Oracle E-Business Suite Data

Oracle STRONGLY RECOMMENDS that you never use SQL*Plus, Oracle Data Browser, database triggers, or any other tool to modify Oracle E-Business Suite 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 E-Business Suite data, you risk destroying the integrity of your data and you lose the ability to audit changes to your data.

Because Oracle E-Business Suite tables are interrelated, any change you make using an Oracle E-Business Suite form can update many tables at once. But when you modify Oracle E-Business Suite data using anything other than Oracle E-Business Suite, 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 E-Business Suite.

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

1

About EGRCM

EGRCM Explained

Worldwide, law makers, regulators and investors are placing increasing mandates on business to improve transparency and controls over financial and compliance reporting. Laws such as the U.S. Sarbanes Oxley Act, Canadian Bill 198, OMB Circular 123A, and Japanese SOX (J-SOX), are forcing organizations to adopt rigorous approaches to documenting and testing internal processes and controls. EGRCM helps reduce the cost and complexity of compliance and to helps organizations leverage their compliance efforts to create new process efficiencies.

EGRCM consists of a set of self-contained, loosely coupled functional modules called Application Modules that collectively provide an integrated system of components necessary to manage the various areas of an organization's Governance, Risk, and Compliance objectives. EGRCM is seeded with a GRC Framework Application Module and a Financial Governance Module. In addition, you can create your own specific components to suite your business needs.

Software Distribution and Language Support

Download EGRCM via E-delivery. Oracle can also supply the product on DVD to accommodate specific customer requests.

The user interface is in American English. The following languages are supported:

- American English
- Chinese – Simplified
- Chinese Traditional
- Danish
- Dutch

- French
- German
- Italian
- Japanese
- Korean
- Portuguese (Brazilian)
- Spanish

About This Guide

This document provides information required to install the EGRCM application on a Linux 5 system.

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 guide is intended for information technology personnel and privileged users responsible for installing and configuring EGRCM.

Conventions

The following conventions are used throughout this guide:

- The notation `<Install_Dir>` / is used to refer to the location on your system where the software is installed.
- Forward slashes (/) are used to separate the directory levels in a path name. A forward slash will always appear after the end of a directory name.

2

Pre-Installation Tasks and Considerations

Requirements

Hardware Requirements

These requirements apply to most installations, assuming 1000-2500 named users and 50-75 concurrent users. The server specifications are typical, but additional analysis might be required to determine your final configuration.

- Hardware Specifications:
  - 2GHz+ processor
  - Dual CPU+
  - 8GB+ RAM
- Application Server: 2 Managed Server JVMs with 1 GB RAM (an additional 500 MB is needed if using optional reporting Managed Server)
- Application Disk Space: 50 GB RAID
- Database Server: 2 GB SGA (with optional reporting, an additional 1 GB is required)
  - Support for Unicode AL32UTF8 character set
- Database Table Space: 200 GB (with optional reporting, an additional 25 GB is required)

Software Requirements

The following software must be installed before you can install EGRCM:

Server Environment:

- Intel x86 64-bit Platform
- Oracle Enterprise Linux 5 (Update 2 or 3) 64-bit
- Oracle Database Server 11gR2 (11.2.0.1.0) 64-bit
- Oracle SOA (Service Oriented Architecture) Suite 11gR1PS1 (11.1.1.2.0) 64-bit, including Enterprise Manager and the Repository Creation Utility (RCU) 11gR1PS1. The following RCU components are required::
  - Metadata Services (MDS schema)
  - SOA Infrastructure (SOAINFRA schema)
  - Business Activity Monitoring (ORABAM schema)
  - User Messaging Service (ORASDPM schema)
- Oracle BI Publisher 10gR3 (10.1.3.4) 64-bit (not required, but available for optional 64-bit reporting solution)
- JRockit Real Time 3.1 for Java SE 6 for Linux x86-64
- Oracle WebLogic Server 11g R1PS1 (10.3.2) 64-bit

  Note: If your database tier is remote to EGRCM you must also install an RDBMS 11g Client to provide SQL*Plus.

- Oracle Internet Directory Release 11.1.1.2.0. For additional information, download the OID Administration Guide and the OID Installation Guide from the Oracle Technology Network (OTN) OID documentation page.

  Note: This is optional, you can use embedded LDAP instead of OID.

Refer to the documentation for each software for installation details.

- Business Intelligence Reporting Requirements

  Refer to the *Oracle Enterprise Governance, Risk and Compliance Manager BI Publisher Reports Installation Guide* for details of installing BI reports.

End User Environment

- Internet Explorer 7 or higher or Firefox 3.

Note: The EGRCM application login page uses the browser locale to determine which language to display. If no browser locale is found, then American English will be used. After login, the language from the User Preferences page is used.

- Adobe Flash plug-in installed
- JavaScript enabled
- Pop-up Blocker disabled for server hosts

3

Installing EGRCM

grc.zip File Explained

The grc.zip contains the following files:

- applications
  - Framework.ear: The Main Enterprise GRCM Application. This application is deployed into the GRC Managed Server (grc_server1).
  - EntityServices.ear: Supporting Web Services Application for the Main EGRCM Application. Updates Entities. Deployed into the SOA Server (soa_server1).
  - DelegationServices.ear: Supporting Web Services Application for the Main EGRCM Application. Provides Delegation Services to the BPEL Composites. Deployed into the SOA Server (soa_server1).
  - OrgPropagationServices.ear: Supporting Web Services Application for the Main EGRCM Application. Deployed into the SOA Server (soa_server1).
  - Ohw-grc.ear: This application provides the online help for OEGRCM
- soa
  - GRCCommonComposite.zip: GRCCommonComposite.zip file contains the common BPEL Composite. This is a SAR file that is deployed into the SOA Server (soa_server1).
  - GRCCommonDelegComposites.zip: GRCCommonDelegComposites.zip file contains the common Delegation BPEL Composite. This is a SAR file that is deployed into the SOA Server (soa_server1).
  - GRCDepComposites.zip: GRCDepComposities.zip file contains all the other

composites used by EGRCM. This is a SAR file that is deployed into the SOA Server (soa_server1).

- scripts
  - grcMasterInstall.py: The Master Installer
  - grcMasterInstallWin.py: The Master Installer for Windows
  - grc_install.properties: The properties file used by the installer
  - GrcInstall.jar: The jar file to support the master installer scripts
  - default-keystore.jks: The default keystore file
  - Ext_getpass.py: Script to support the master installer script
  - oid_group.ldif: This is the file for loading the groups into OID. There are additional files for loading the groups in languages other than english
- reports
  - reports.zip : This is the file for the optional reporting installation. Refer to the *Oracle Enterprise Governance, Risk and Compliance Manager BI Publisher Reports Installation Guide* for details.
- db
  - fgrcmSchema.sql: The Master SQL file that contains all the EGRCM Object Definition.
- README.txt
- Other Seed and Metadata SQL files
  - fgrcmSchema.sql
  - seed_actv_dir_actv.sql
  - seed_actv_dir_resps.sql
  - seed_attachmentServer.sql
  - seed_fnd_currencies.sql
  - seed_fnd_currencies_tl.sql
  - seed_grc_actions.sql

- seed_grc_actions1_tl.sql
- seed_grc_actions2_tl.sql
- seed_grc_actv_dir_actv_tl.sql
- seed_grc_actv_dir_resps_tl.sql
- seed_grc_analysis_params.sql
- seed_grc_analysis_params_tl.sql
- seed_grc_association_display.sql
- seed_grc_associations.sql
- seed_grc_cfg_param_assign.sql
- seed_grc_config_features.sql
- seed_grc_content_types.sql
- seed_grc_content_types_tl.sql
- seed_grc_dashboard_graphs_xref.sql
- seed_grc_delegation_matrix_rules.sql
- seed_grc_delegation_model0_setup.sql
- seed_grc_delegation_model1_risk.sql
- seed_grc_delegation_model2_control.sql
- seed_grc_delegation_model3_component.sql
- seed_grc_delegation_model4_issue.sql
- seed_grc_delegation_model5_perspective.sql
- seed_grc_delegation_model6_asmt_result.sql
- seed_grc_delegation_model6_assessment.sql
- seed_grc_delegation_model7_survey.sql
- seed_grc_delegation_model_tl.sql

- seed_grc_graph_definitions.sql
- seed_grc_graph_definitions_tl.sql
- seed_grc_impact_models.sql
- seed_grc_impact_models_param_xrefs.sql
- seed_grc_impact_models_tl.sql
- seed_grc_instance5_perspective_data1.sql
- seed_grc_instance5_perspective_data1b.sql
- seed_grc_instance5_perspective_data2.sql
- seed_grc_instance5_perspective_data2b.sql
- seed_grc_instance5_perspective_data2c.sql
- seed_grc_instance_data.sql
- seed_grc_instance_perspective_tl.sql
- seed_grc_languages.sql
- seed_grc_languages_tl.sql
- seed_grc_likelihood_models.sql
- seed_grc_likelihood_models_tl.sql
- seed_grc_likelihood_param_xrefs.sql
- seed_grc_lookups.sql
- seed_grc_lookups_tl.sql
- seed_grc_module_definitions.sql
- seed_grc_module_definitions_tl.sql
- seed_grc_module_roles.sql
- seed_grc_module_udt_xrefs.sql
- seed_grc_ObjectClasses.sql

- seed_grc_object_classes_tl.sql
- seed_grc_object_guide_texts.sql
- seed_grc_object_guide_tl.sql
- seed_grc_object_type_configs.sql
- seed_grc_object_type_features.sql
- seed_grc_ObjectTypes.sql
- seed_grc_object_types_tl.sql
- seed_grc_ObjectTypeTree.sql
- seed_grc_page_compositions.sql
- seed_grc_page_definitions.sql
- seed_grc_page_graphs_xref.sql
- seed_grc_question_format_types.sql
- seed_grc_risk_analysis_model.sql
- seed_grc_risk_analysis_model_tl.sql
- seed_grc_risk_context_model.sql
- seed_grc_risk_context_model_tl.sql
- seed_grc_risk_significance_model.sql
- seed_grc_risk_significance_model_tl.sql
- seed_grc_setup_maintenance.sql
- seed_grc_setup_maintenance_tl.sql
- seed_grc_state_access_actns.sql
- seed_grc_state_access_actns1_perspective.sql
- seed_grc_state_access_actns3_component.sql
- seed_grc_state_access_actns4_issue.sql

- seed_grc_state_access_actns_consequence.sql
- seed_grc_state_access_actns_events.sql
- seed_grc_state_access_actns_proposedrisk.sql
- seed_grc_state_access_actns_risk.sql
- seed_grc_state_access_actns_riskanalysis.sql
- seed_grc_state_access_actns_riskevaluation.sql
- seed_grc_state_access_actns_suvtemplate.sql
- seed_grc_state_access_attr.sql
- seed_grc_state_access_attr1_perspective.sql
- seed_grc_state_access_attr3_component.sql
- seed_grc_state_access_attr4_issue.sql
- seed_grc_state_access_attr_risk.sql
- seed_grc_state_access_attr_suvtemplate.sql
- seed_grc_survey_choices.sql
- seed_grc_survey_choiceset.sql
- seed_grc_survey_choiceset_tl.sql
- seed_grc_survey_choices_tl.sql
- seed_grc_survey_question_format_tl.sql
- seed_grc_survey_templates_questions.sql
- seed_grc_survey_templates_questions_tl.sql
- seed_grc_territories.sql
- seed_grc_territories_tl.sql
- seed_grc_uda.sql
- seed_grc_uda_tl.sql

    - to_be_deleted.sql
    - user_create.sql
- templates
    - oracle.grc_template_11.1.1.jar: The Weblogic Domain template for the EGRCM Managed Server
    - oracle.grc_bip_template_11.1.1.jar: The Weblogic Domain template for the BIP Managed Server

Pre-Installation Tasks

Perform the following steps before you begin your install, you must:

1. Install the Oracle 11g Database.
2. Install JRockit Real Time 3.1.
3. Run rcu to install SOA schemas.
4. Install Weblogic.
5. Install SOA Suite.
6. Run the Domain Configuration wizard to create a domain.

You must also perform the following system configuration tasks before you can begin the EGRCM install:

- Because the install script uses the jar utility to extract the files and modify the connection parameters, you must ensure that the jar utility is in the search path.
- Because the install script uses sqlplus to connect to an Oracle database to execute the sql scripts, you must ensure that sqlplus is in the search path.
- The install script modifies the domain. In order to restore the original domain, backup the user_projects directory under middleware home. For example, you can backup this directory using the command:

  ```
  tar cvf user_projects.tar user_projects
  ```

- Unzip grc.zip under $MW_ORA_HOME. If you have unzipped the grc.zip elsewhere, move it to $MW_ORA_HOME.
- Carefully populate the property values in the grc_install.properties file. The properties are described in the comments of the grc_install.properties file.

If you are using optional reporting, you must set up the properties used for creating the data source for communication between EGRCM application and Oracle Data Integrator. If you do not set these properties during EGRCM install, you can do so manually using the Weblogic console later as follows:

1. Log in to the weblogic console.
2. Navigate to Domain > Services > JDBC > Data Sources
3. Create a new Data Source as follows:
    - Name: grcDS
    - JNDI name: jdbc/grcDS
4. Follow through the wizard to create the data source. This data source must point to your Oracle Data Integrator user repository. Make sure that the data source is targeted to your grc server. For additional details on creating data sources, refer to the Weblogic documentation.

- Set the following environment Variables:
    - MW_HOME to your Middleware Home, for example: MW_HOME=/home/grc/Oracle/MW5536RC3
    - MW_ORA_HOME to your SOA HOME for example: MW_ORA_HOME=$MW_HOME/AS11GR1SOA
    - For Windows and Solaris installations, set CLASSPATH to $MW_ORA_HOME/GrcInstall.jar
    - JAVA_VENDOR to Sun, for example: JAVA_VENDOR=Sun
    - USER_MEM_ARGS to –Xms512m –Xmx1024m –XX:CompileThreshold=8000 –XX:Permsize=512m –XX:MaxPermSize=1024m
    - NLS_LANG to AMERICAN_AMERICA.AL32UTF8
- Create a database schema user/owner (for example, GRC). The database user should have the following privileges:
    - resource
    - connect
    - create view
    - create synonym

- create any context
- drop any context

In addition to creating a database user, you also must create GRC_APP_CONTEXT with the following command:

```
create context GRC_APP_CONTEXT using grc_security_pkg;
```

A sample script is provided to create GRC user and schema with the required privileges. The script also creates the GRC_APP_CONTEXT. Execute the script grc/db/user_create.sql as sysdba. If you use the script to create a user that is different than GRC user, you must update the script and replace the GRC user with the user you want to create.

Context Configuration to Install Multiple EGRCM Application Schemas on One Database Instance: To create multiple GRC users (for example, GRC1 and GRC2 on the same database instance, after you create the GRC users (GRC1 and GRC2), perform the following steps:

1. Create a new user GRC_CONTEXT on the same database instance, and install the grc_security_package and all dependancies. The simplest way to do this is to modify the user_create.sql to create the GRC_CONTEXT user. Then, connect to the user and run the fgrcmSchema.sql script to create packages.

2. Create synonyms for grc_security_package for all the GRC users. For example:

   Example

   SQL> connect GRC1/[password];

   SQL> create synonym grc_security_pkg for GRC_CONTEXT.grc_security_pkg;

   SQL> connect GRC2/[password];

   SQL> create synonym grc_security_pkg for GRC_CONTEXT.grc_security_pkg;

3. Connect to GRC_CONTEXT, create context and grant executes permission to all the GRC users. For example:

   Example

   SQL> create context grc_app_context using grc_security_pkg;

   SQL> grant execute on grc_security_pkg to GRC1;

   SQL> grant execute on grc_security_pkg to GRC2;

Installation Tasks

1. Make sure that the admin server and SOA server are not running.

2. Navigate to the GRC script directory. For example:

cd $MW_ORA_HOME/grc/scripts

3. Execute the Install script using one of the following commands:

   - For Linux installations:

     ```
     $MW_ORA_HOME/common/bin/wlst.sh ./grcMasterInstall.py
     ```

   - For Windows installations:

     ```
     $MW_ORA_HOME/common/bin/wlst.sh ./grcMasterInstalWin.py
     ```

   - For Solaris installations:

     ```
     $MW_ORA_HOME/common/bin/wlst.sh ./grcMasterInstalSolWin.py
     ```

   Ensure that the terminal on which you are running the install has sufficient scroll-back lines (for example, 5000) to capture all the output from the install activities. This allows you to review all the install activities later.

   > **Important:** The install script attempts to start the Admin Server. It tests in a loop if the server is up before it continues. If you installed your WebLogic Server in Production Mode, the Admin server requires a userid and password to start which the script does not set for security reasons. In this case, you must start a new terminal window to start the Admin Server. Once the script detects the server has started, it will continue.

4. Make sure the environment variables are set as described in the Pre-Installation tasks, then navigate to $MW_HOME/user_projects/domains/base_domain. Issue the following commands in separate terminals to the managed servers soa_server1 and grc_server1:

   ```
   Sh bin/startManagedWebLogic.sh soa_server1
   ```

   ```
   Sh bin/startManagedWebLogic.sh grc_server1
   ```

   Once the managed servers are started, press enter in the first terminal where grcMasterInstall.py is run.

5. The EGRCM installation output is captured in the scroll buffer of the terminal on which you run the installation. Scroll through the buffer to check for errors. Ignore the following warning messages:

   - `sed: can't read -: No such file or directory`

   - ```
     Error starting at line 1 in command: CREATE FORCE VIEW
     ........
     ```

     ```
     ...... Error report: SQL Command: CREATE FORCE Failed:
     Warning: execution completed with warning
     ```
     ```

6. Deploy Oracle BI Publisher to the BIP Server. Refer to the *Oracle Enterprise Governance, Risk and Compliance Manager BI Publisher Reports Installation Guide* for details.

Post Installation Tasks

Perform the following steps after the install:

1. To configure the EGRCM application SOA and web services security, you must create and setup your keystore as follows:
    1. Use keytool to set up your keystore using the following command:

        ```
        keytool -genkeypair -alias orakey -keyalg "RSA" -keystore
        default-keystore.jks -validity 3600
        ```

    2. When prompted, enter your keystore password and key password. This creates a keystore called default-keystore.jks and a key pair with the alias orakey within that keystore.

    3. Move the keystore that you just generated to the fmwconfig directory. For example:

        ```
        mv default-keystore.jks
        <user_projects>/<domains>/<base_domain>/config/fmwconfig
        ```

        This overwrites the default-keystore.jks file. Refer to the Setting up the Keystore for Message Protection section of the*Oracle Fusion Middleware Security and Administrator's Guide* for additional details.

2. Use Enterprise Manager (EM) to setup credentials after the Keystore is setup as follows:
    1. Access your EM at:

        ```
        http://<ServerName>:<admin port>/em
        ```

    2. Click on Weblogic Domain> base_domain

    3. Right click on the base_domain and select Security > Credentials

    4. On the Credentials page:
        - Click on the '+ Create Map' button
        - Enter: oracle.wsm.security as the Map Name
        - Click OK

        A new row, oracle.wsm.security is created.

5. Click the **+ Create Key** button to add keys in the wallet. When prompted, enter the key information as follows, depending on your keystore:

    1. basic.credentials: This contains the user authentication (User and Password used for the UserNameToken)

        - Select Map - oracle.wsm.security
        - Key - basic.credentials
        - Type - Password
        - Username - *weblogic username*
        - Password - *password*
        - Description - User credentials key

    2. keystore-csf-key

        - Select Map - oracle.wsm.security
        - Key - keystore-csf-key
        - Type - Password
        - Username - owsm
        - Password - *keystore password*
        - Description - Keystore key

    3. enc-csf-key

        - Select Map - oracle.wsm.security
        - Key - enc-csf-key
        - Type - Password
        - Username - orakey
        - Password - *orakey password*
        - Description - Encryption key

    4. sign-csf-key

- Select Map - oracle.wsm.security
- Key - sign-csf-key
- Type - Password
- Username - orakey
- Password - *orakey password*
- Description - Signing key

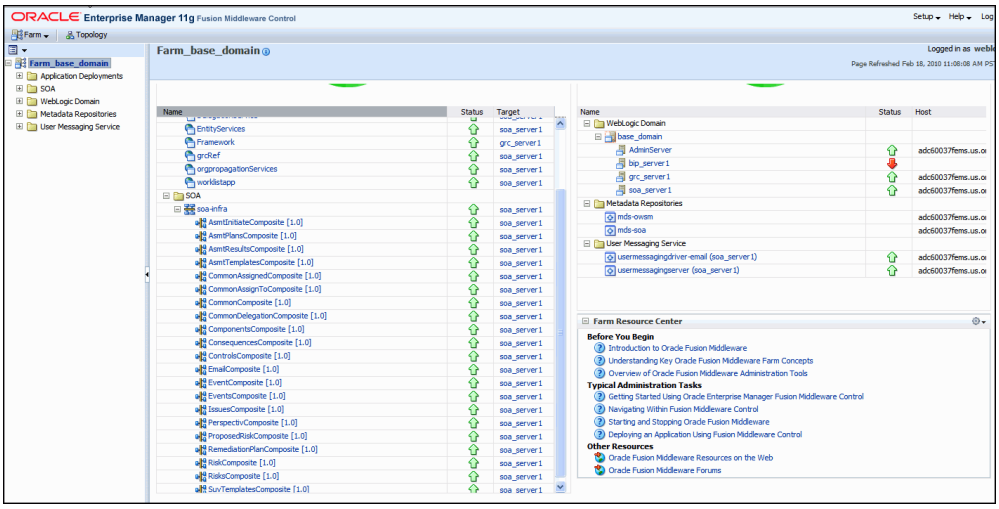
For additional details, refer to the Manage the Credential Store Framework Section of the *Securing WebLogic Web Services for Oracle WebLogic Server* guide.

After installation is complete your domain should be running with at least the following:

- AdminServer
- SOA Server
- GRC Server
- BIP Server - You will have an additional BIP Server if you opted to install optional reporting.

To verify that the servers are running:

1. Login to Enterprise Manager 11g.
2. Select the appropriate domain from the WebLogic Domain folder.
3. The current statuses are displayed. For example:



The SOA server will have all the GRC composites marked as active. All of the web services are targeted to the SOA server and they should be marked as active. The EGRCM application called Framework should be targeted to the GRC server and should be marked as active. There should be a grc DS JDBC Data Source that should be targeted to all the three above mentioned servers.

The following are helpful URLs:

- WLS (Weblogic Server) Console: http:/<adminHost>:<adminPort>/console
- EM (Enterprise Manager) Console: http://<adminHost>:<adminPort>/em
- WorklistApp: http://<soaHost>:<soaPort>/integration/worklistapp
- EGRCM: http://<grcHost>:<grcPort> /GRCApp/faces/oracle/apps/grc/framework/tools/page/GRCLandingPG.jspx

Note: After completing all post installation tasks, you must create a valid EGRCM user and associate relevant roles to the user as described in the Creating Users and Enterprise Groups in Embedded LDAP, page 4-1 section of this guide.

Note: During the installation process there are seven database views that are dependent on other database views. Because of the order of execution, the database views have the "Force Create" option enabled. This causes the database views to be created when the dependent views have not yet been created. In some cases, database tools such as SQL Developer identify these database views as invalid. In actuality, the database views are created correctly and data is selected correctly by the application. If you receive these warnings during the installation

process, you can use a database tool such as SQL Developer to compile the database views. This removes the warning messages. The database views with the Force Create option enabled are:

- GRC_ACTV_OBJ_ICONS_VL
- GRC_ASMT_BPELRSLTS_V
- GRC_COMPONENT_MATRIX_VL
- GRC_CURR_BASE_UDTS_VL
- GRC_CURR_UDT_CLASS_VL
- GRC_CURRENT_ACTVS_VL
- GRC_ISSUE_COUNT_VL

Reinstallation Tasks

In the event that an installation fails, follow this procedure to perform a new installation:

1. Make sure that the environment variables are set as described in Pre-Installation Tasks, page 3-7, and that you are in $DOMAIN_HOME (typically $MW_HOME/user_projects/domains/base_domain)

2. Stop the SOA Server. Go to $DOMAIN_HOME and issue the following commands at the prompt:

   ```
   sh bin/stopManagedWebLogic.sh soa_server1
   ```

   For example: `sh bin/stopManagedWebLogic.sh soa_server1 t3://host.oracle.com:7001`

3. Stop the GRC Server. Go to $DOMAIN_HOME and issue the following commands at the prompt:

   ```
   sh bin/stopManagedWebLogic.sh grc_server1
   ```

4. Stop the BIP Server. Go to $DOMAIN_HOME and issue the following commands at the prompt:

   ```
   sh bin/stopManagedWebLogic.sh bip_server1
   ```

5. Stop the Admin Server. Go to $DOMAIN_HOME and issue the following command at the prompt:

   ```
   sh bin/stopManagedWebLogic.sh
   ```

6. Perform cleanup tasks:
    1. Clean up the $MW_HOME/user_projects directory and restore from the backup taken before the initial installation.
    2. Delete the grc directory under $MW_ORA_HOME
    3. Delete oracle.grc_template_11.1.1.jar and oracle.grc_bip_template_11.1.1.jar from $MW_ORA_HOME/common/templates/applications directory
    4. If you are performing a database schema and seed data install (that is, the DbInstall property was marked as "yes" in the grc_install.properties file) then you must clean up the database. Delete the database user you created before and all related objects using the cascade option. For example:

       DROP USER [username] CASCADE;
7. Follow the steps for a new install.

Enabling Additional Languages

EGRCM is installed with American English as the base language. Follow these steps to enable additional languages.

1. Login to sqlplus as the grc user.
2. At the prompt, enter:

   ```
   exec grc_languages_pkg.add_language('target_language');
   ```

   For example to enable German, enter:

   ```
   exec grc_languages_pkg.add_language('D');
   ```

The available additional language codes are:

- D (German)
- DK (Danish)
- E (Spanish)
- F (French)
- I (Italian)
- JA (Japanese)
- KO (Korean)

- NL (Dutch)
- PTB (Brazilian Portuguese)
- ZHS (Simplified Chinese)
- ZHT (Traditional Chinese)

4

Security

Security Explained

There are two types of security:

- Functional security is a statement of what you can do. It typically mirrors what you would see on a job description. For example, a Risk Manager is responsible for creating and maintaining the definitions of risks, events, consequences and risk models.
- Data Security is a statement of what action can be taken against which data. For example, a Risk User can only edit risks that they own, and only before they are approved.

Creating Users and Groups

There are two ways you can manage users and groups:

- Use Embedded LDAP, page 4-1
- Use Oracle Internet Directory, page 4-2

Creating Users and Enterprise Groups in Embedded LDAP

Follow this procedure to create new users and Enterprise groups:

1. Navigate to the WebLogic server administration Console:

   http://<HostName>:<portno>/console

2. Click on the Security Realms link. The Summary of Security Realm is displayed.
3. Click on the myrealm link in the "Summary of Security Realms" region. The

myrealm settings page is displayed.

4. Click on the Users and Groups Tab. A list of existing users is displayed.

5. Click on the New Button. The user creation page is displayed.

6. Enter a name, description and password for the user. Note that the name is what the user will enter when they login, and the description is how the user is displayed in lists of values.

   Tip: Use an LDAP browser (such as JExplorer LDAP) to add an e-mail address to the user definition. This is the e-mail address that is used when sending notifications.

7. Click OK.

8. Click on the username that you just created.

9. Click the Groups tab.

10. Assign one or more job roles to the user.

11. Click Save.

12. Enterprise groups map to job, abstract and data roles. To create an enterprise group, click on the Groups Tab. A page showing all existing groups is displayed

13. Click OK.

14. Click on the New Button. The Enterprise Group creation page is displayed.

15. Fill in the group details and leave everything else as default.

    Note: You must suffix Enterprise group names with "_Job_Role".

16. Click OK when done.

Configuring EGRCM for OID

You can optionally configure Oracle Internet Directory to be your authentication provider instead of the default option of using embedded LDAP. If you decide to use OID instead of embedded LDAP, you must perform the following configuration steps:

1. Upload oid_groups.ldif, which contains the Enterprise roles, using the following command:

   ```
   ldapadd -h ldap_host -p ldap_port -D cn=orcladmin -w password
   ```

```
-c -v -f ldif file name
```

Note: oid_groups.ldif is in the directory "scripts" in the grc.zip file.

2. Create an OID Authenticator in WLS as follows:
   1. Log into Weblogic Console.
   2. Navigate to: SecurityRealms\[Default Realm Name]\Providers
   3. Click New, then select "OracleInternetDirectoryAuthenticator" from the drop down.
   4. Name the authenticator. For example, OID Authenticator.
   5. Click the newly added authenticator to see the configuration screen for OID Authenticator.
   6. Set the Control Flag to REQUIRED.
   7. Click the Provider Specific tab and configure the following required settings:
      - hosted env OID:
      - host: [OID Host name]
      - port: [OID Port]
      - bind DN: [DN Name] For example, cn=orcladmin
      - password: [Password]
      - User and group base: [user and group base] For example, dc=us,dc=oracle,dc=com
      - User name attribute: uid
      - All users filter: Set as "(&(uid=*)(objectclass=person))"
   8. Save the settings.
3. Change an attribute in Default Authenticator as follows:
   1. Click "Default Authenticator" to see the configuration screen for Default Authenticator.
   2. Set the Control Flag to SUFFICIENT

3. Save the settings.

4. Reorder the Providers as follows:
    1. Navigate to the Providers.
    2. Re-order the Providers as follows:

```
OID Authenticator (REQUIRED) > Default Authenticator
(SUFFICIENT)
```

5. Restart the Admin and the Managed Servers as follows:
    1. Restart the Admin and the Managed Servers.
    2. Navigate to Security Realms > [Default Realm] and click on Users and Groups. You should see users and groups from OID.

For additional details, refer to the Oracle Internet Directory documentation.

Creating Groups or Users in OID

There are multiple ways of managing users and groups in Oracle Internet Directory (OID):

- Import as an LDIF file using bulk load tools
- Use command line tools like ldapadd and ldapmodify
- Use the Oracle Directory Manager (ODSM) tool to create users in OID. ODSM is installed as part of the OID/OAM install.

    Tip: Use an LDAP browser (such as JExplorer LDAP) to add an e-mail address to the user definition. This is the e-mail address that is used when sending notifications.

Refer to the *Oracle Internet Directory Administrator's Guide*, which you can download from OTN, for details.

Configuring EGRCM Single Sign-on Using OAM and OID

1. Create an OID Authenticator in WLS as follows:
    1. Log into Weblogic Console.
    2. Navigate to: SecurityRealms\[Default Realm Name]\Providers

3. Click New, then select "OracleInternetDirectoryAuthenticator" from the drop down.

4. Name the authenticator. For example, OID Authenticator.

5. Click the newly added authenticator to see the configuration screen for OID Authenticator.

6. Set the Control Flag to SUFFICIENT.

7. Click the Provider Specific tab and configure the following required settings:
   - hosted env OID:
   - host: [OID Host name]
   - port: [OID Port]
   - bind DN: [DN Name] For example, cn=orcladmin
   - password: [Password]
   - User and group base: [user and group base] For example, dc=us,dc=oracle,dc=com
   - User name attribute: uid
   - All users filter: Set as "(&(uid=*)(objectclass=person))"

8. Save the settings.

2. Create OAM ID Asserter as follows:
   1. Log into Weblogic Console.
   2. Navigate to SecurityRealms\[Default Realm Name]\Providers.
   3. Click New, then select OAM Identity Asserter from the drop down.
   4. Name the asserter. For example, OAM ID Asserter.
   5. Click the newly added asserter to see the configuration screen for OAM Identity Asserter.
   6. Set the Control Flag to REQUIRED.
   7. Save the settings.

3. Reorder the Providers as follows:

    1. Navigate to the Providers.

    2. Re-order the Providers as follows:

       ```
       OAM Identity Asserter (REQUIRED) >OID Authenticator
       (SUFFICIENT) > Default Authenticator (SUFFICIENT)
       ```

4. Restart the Admin and the Managed Servers as follows:

    1. Restart the Admin and the Managed Servers.

    2. Navigate to Security Realms > [Default Realm] and click on Users and Groups. You should see users and groups from OID.

5. Create Policies in OAM.

    To create Policies in OAM, the following are required:

    - The URL pattern to protect. In this case it is /GRCApp

    - The Host and Port the WebGate to redirect the requests to. In this case, the host of the Managed Server (for example, `servername.mycompany.com`) and port (for example, `8211`.)

    With this information, the OAM administrator is able to create the policies for SSO. Thus, the final URL for the APP is:

    ```
    http://[WebGate Host]:[WebGate
    Port]/GRCApp/faces/oracle/apps/grc/framework/tools/page/GRCLa
    ndingPG.jspx
    ```

For additional details, refer to the Oracle Identity Management documentation.

Jobs, Duties and Application Roles Explained

A job is the actual job description, such as you would see on a job board. Duties are the tasks that the job owner performs. Application roles are collections of duties that job owners perform. Only application roles may be the beneficiary of a permission grant. For example:

- Job: Responsible for managing risk policies and performing complex activities related to business risk analysis. Analyze and manage risks, administer corrective action and protect the business from losses resulting from lack of compliance with consumer laws, regulations and company policy.

- Duties: Completing assessments, GRC reporting, completing GRC Analyses

- Roles: Risk Manager, Risk Administrator

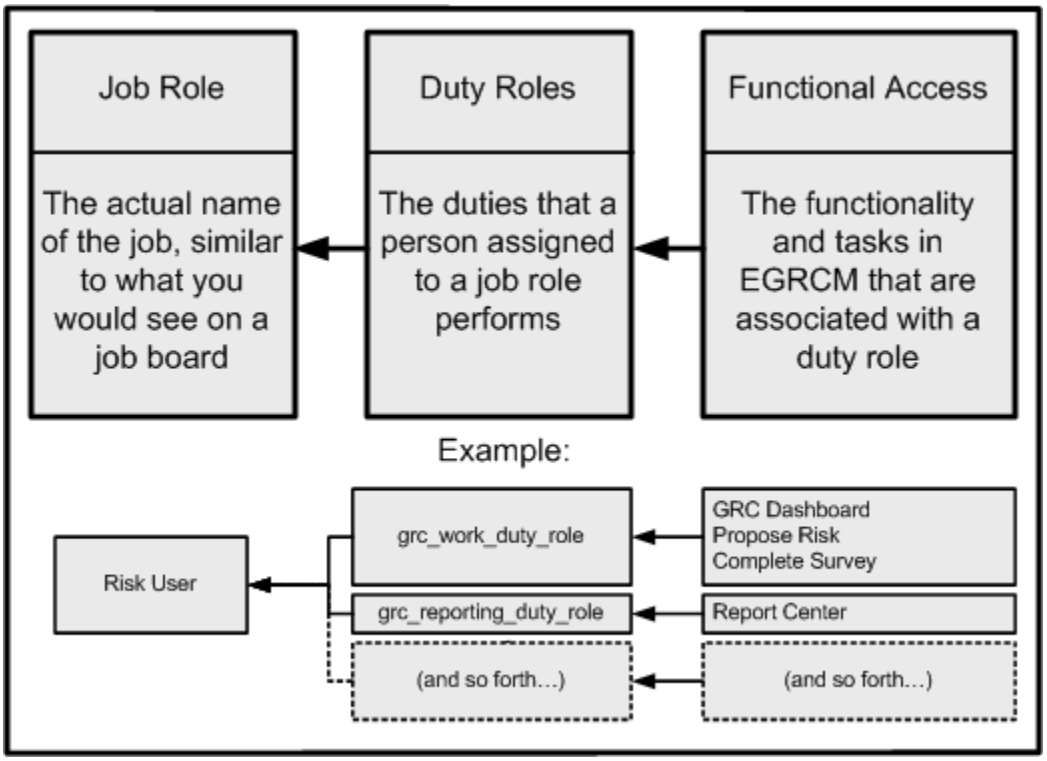
Roles Explained

All users are assigned specific roles that allow them to perform only those tasks that are appropriate to their job. This provides security as only users that are assigned certain roles are allowed to perform certain tasks and to access certain data. Administrators can create roles and users as needed. Note that all job roles must be suffixed with "_Job_Role", for example, Risk_Management_Job_Role.

There are three basic types of job roles:

- Users can perform basic activities (such as viewing or assessing) on existing objects.
- Managers can perform the tasks that a user can, and in addition can also create and manage objects.
- Administrators perform administrative tasks such as creating object classes, plans or models.

Each Job Role has Duty roles that are associated to it. Access to functionality is determined by the Duty Role. For example:



Summary of Seeded Roles

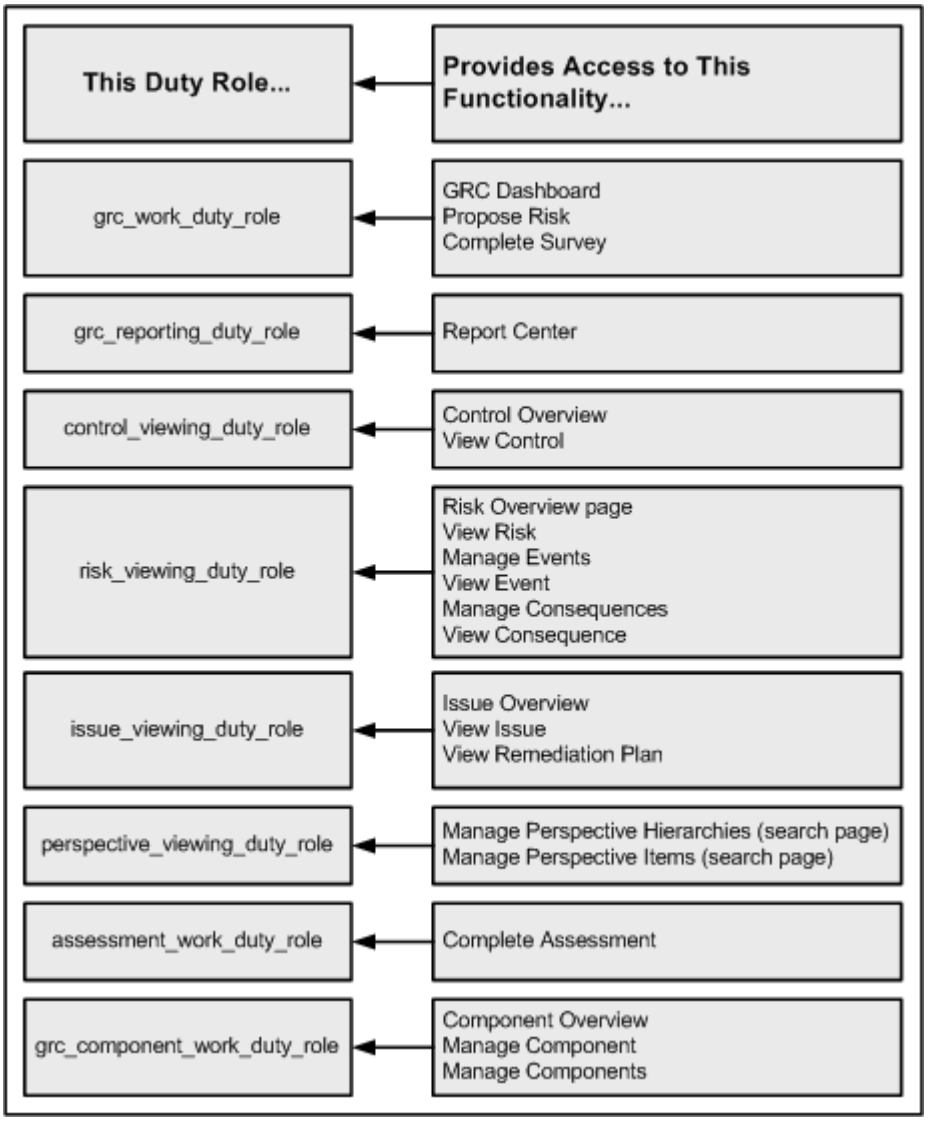
The following roles are seeded in EGRCM.

Note: Administrators see the job role code when they create users in LDAP.

- **CXO**

  Job Role Code: CXO_Job_Role

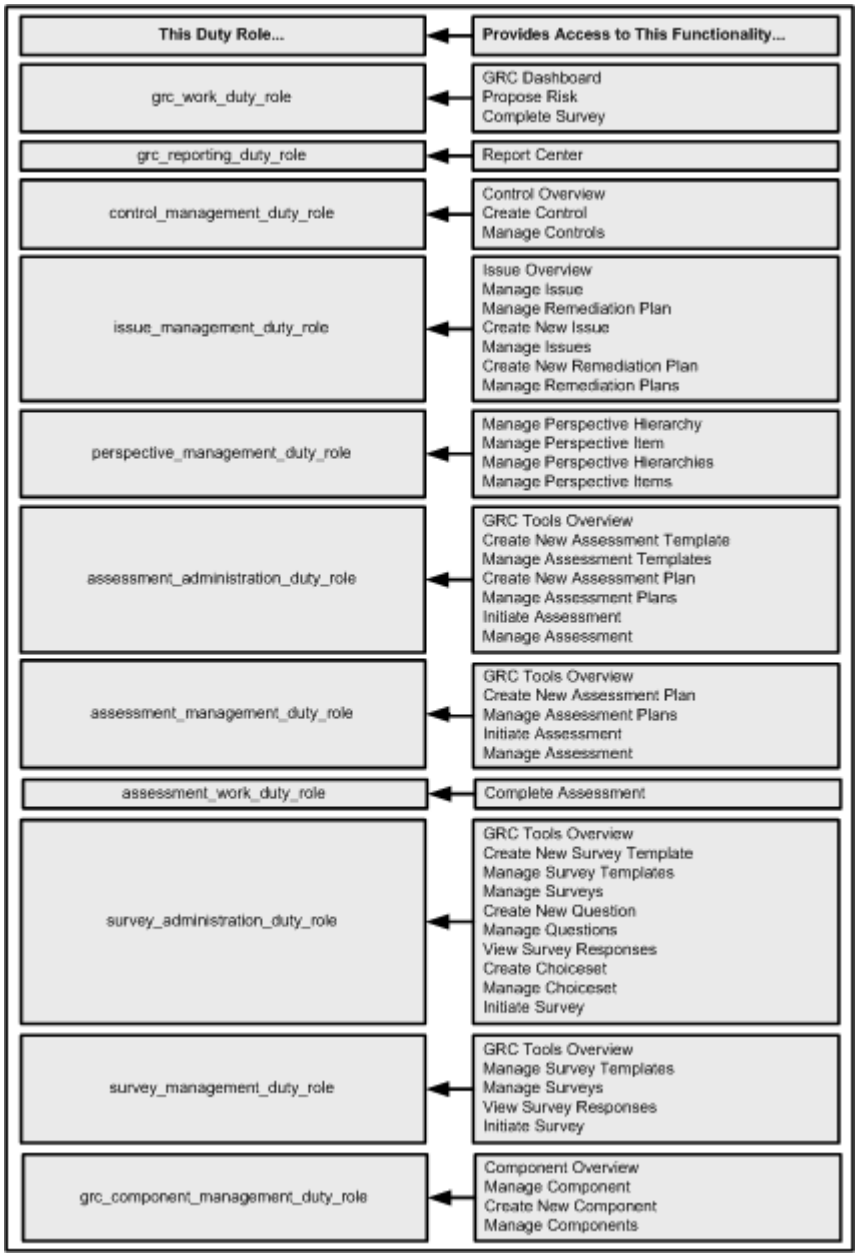
  Duty Roles:



- **IT Controls Manager**

  Job Role Code: IT_Controls_Manager_Job_Role

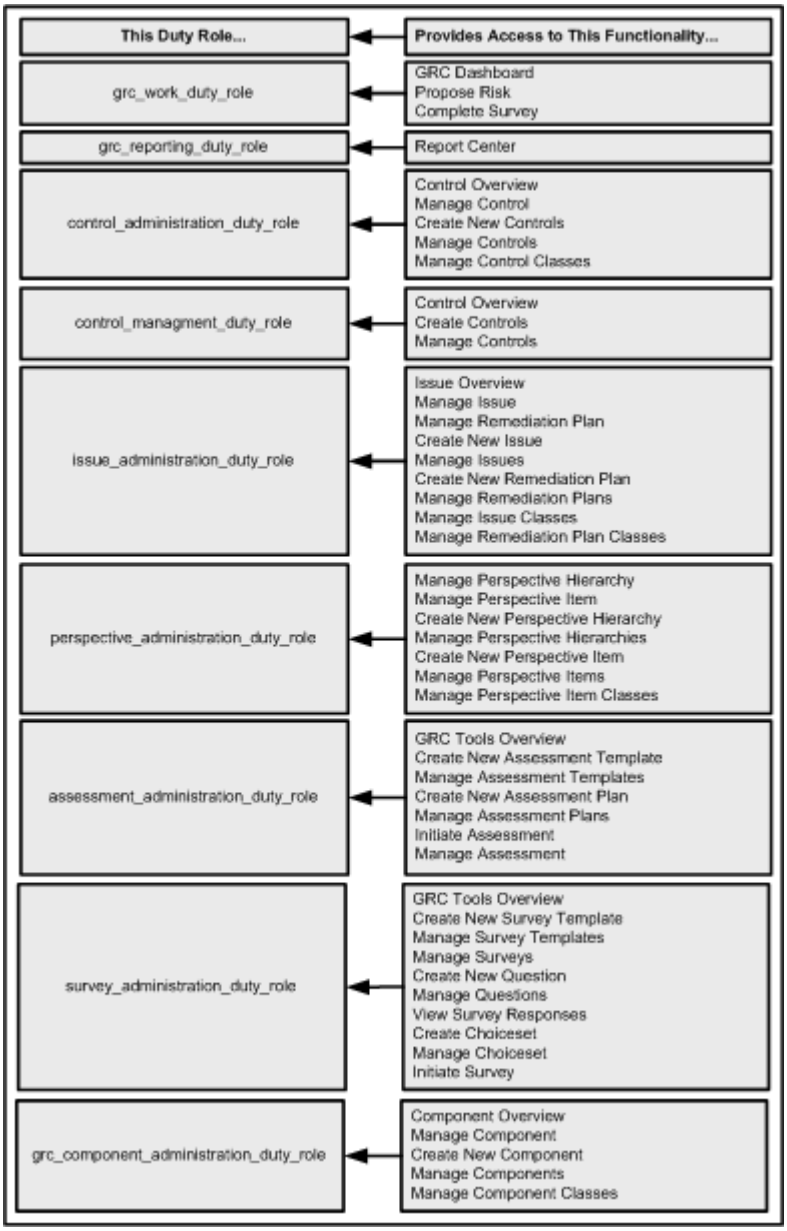
  Duty Roles:



- **Internal Controls Administrator**

  Job Role Code: Internal_Controls_Administrator_Job_Role

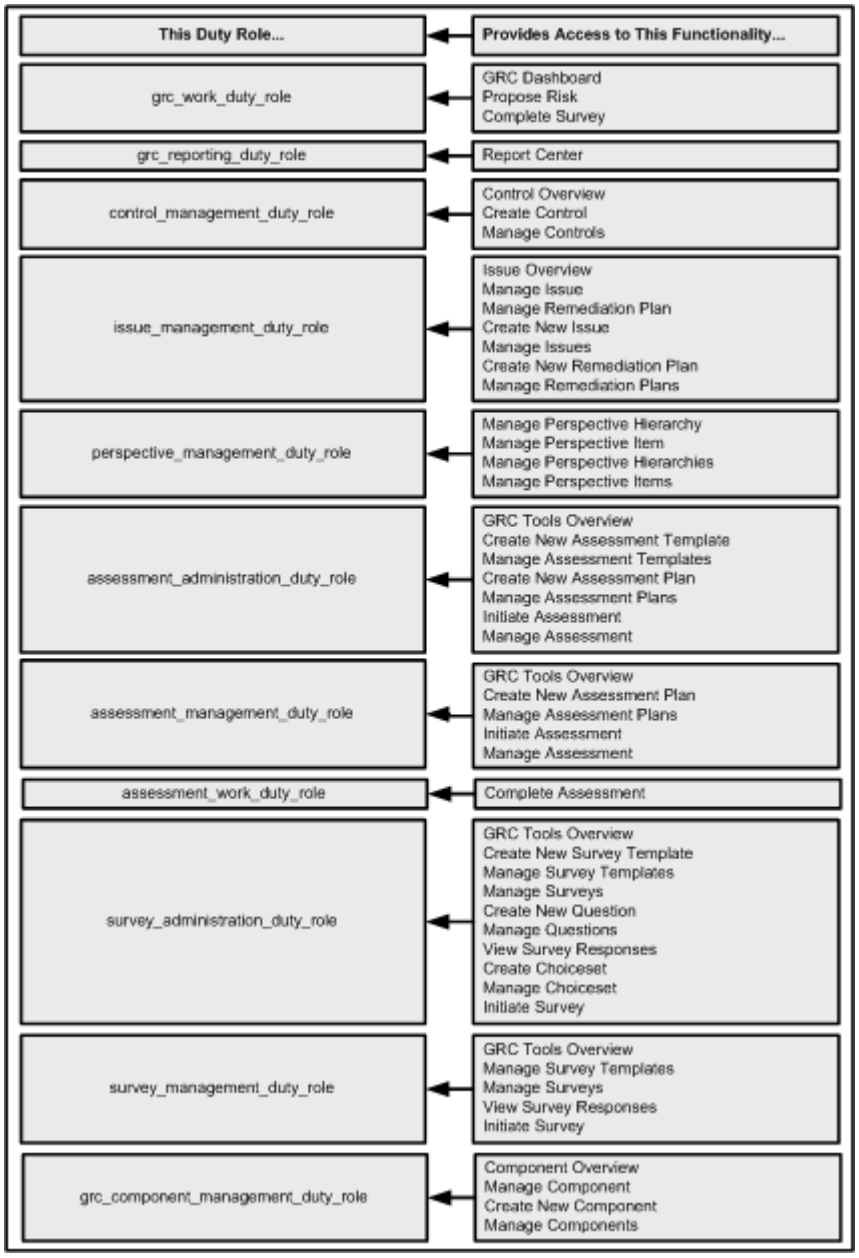
  Duty Roles:



- **Internal Controls Manager**

  Job Role Code: Internal_Controls_Manager_Job_Role

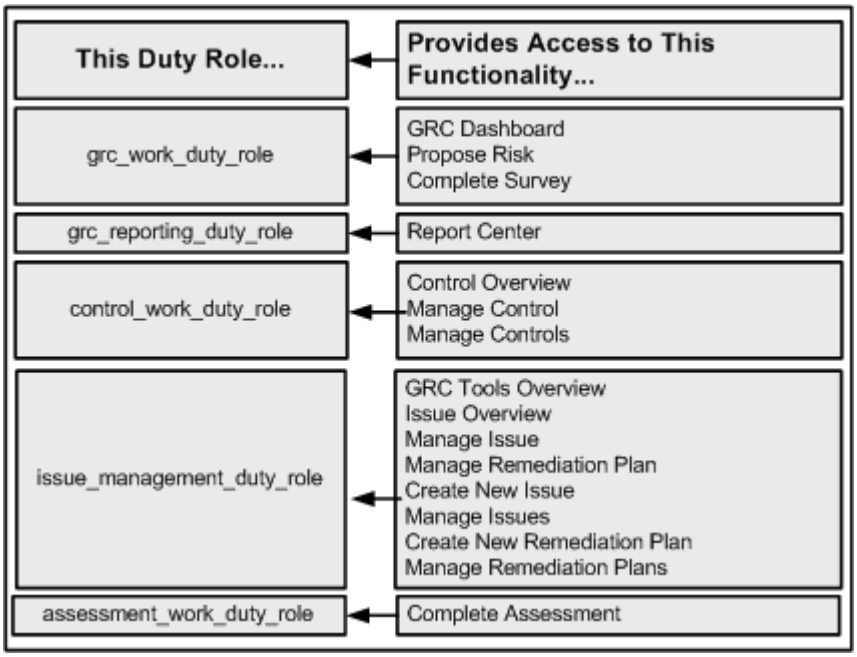
  Duty Roles:



- **Internal Controls User**

  Job Role Code: Internal_Controls_User_Job_Role

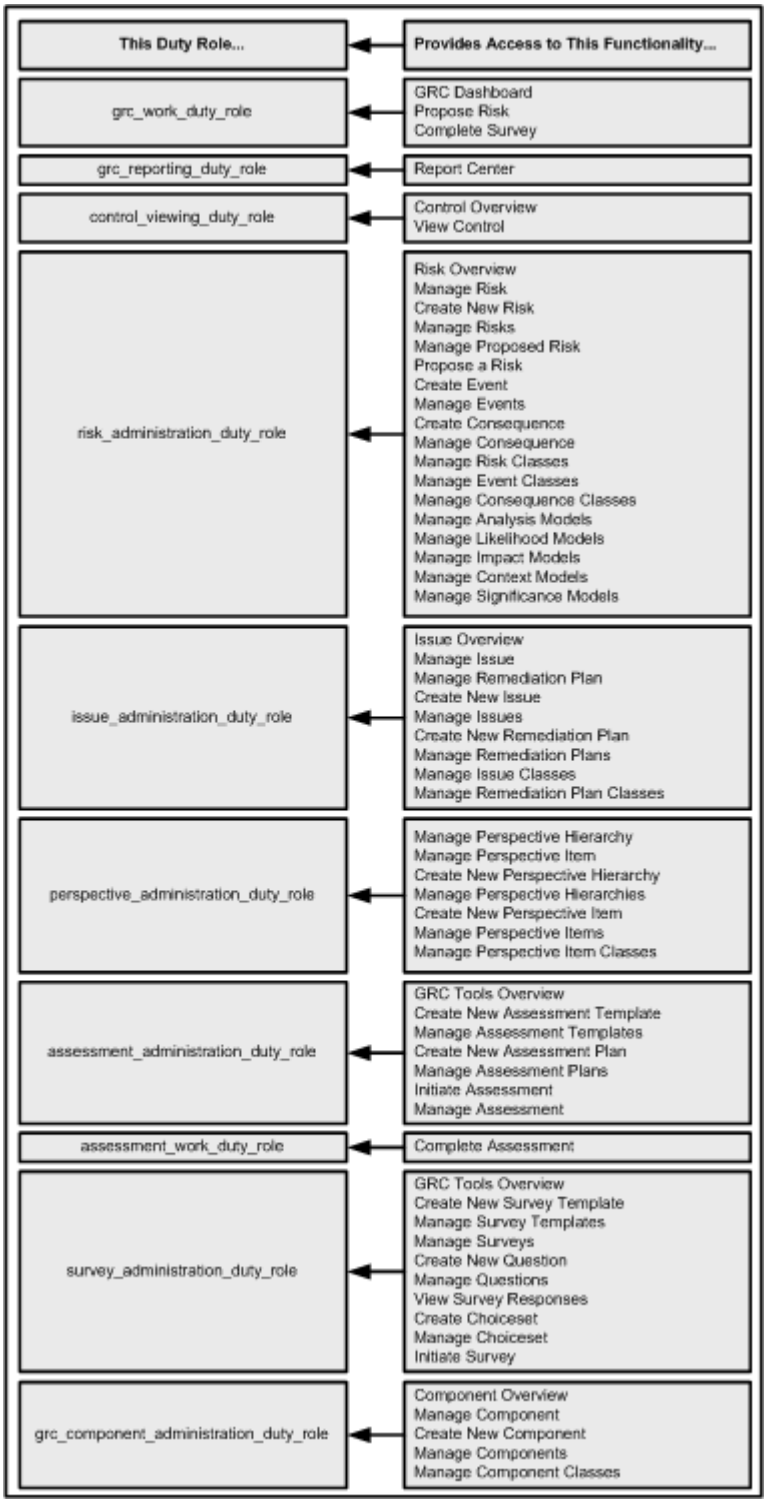
  Duty Roles:



- **Risk Administrator**

  Job Role Code: Risk_Administrator_Job_Role

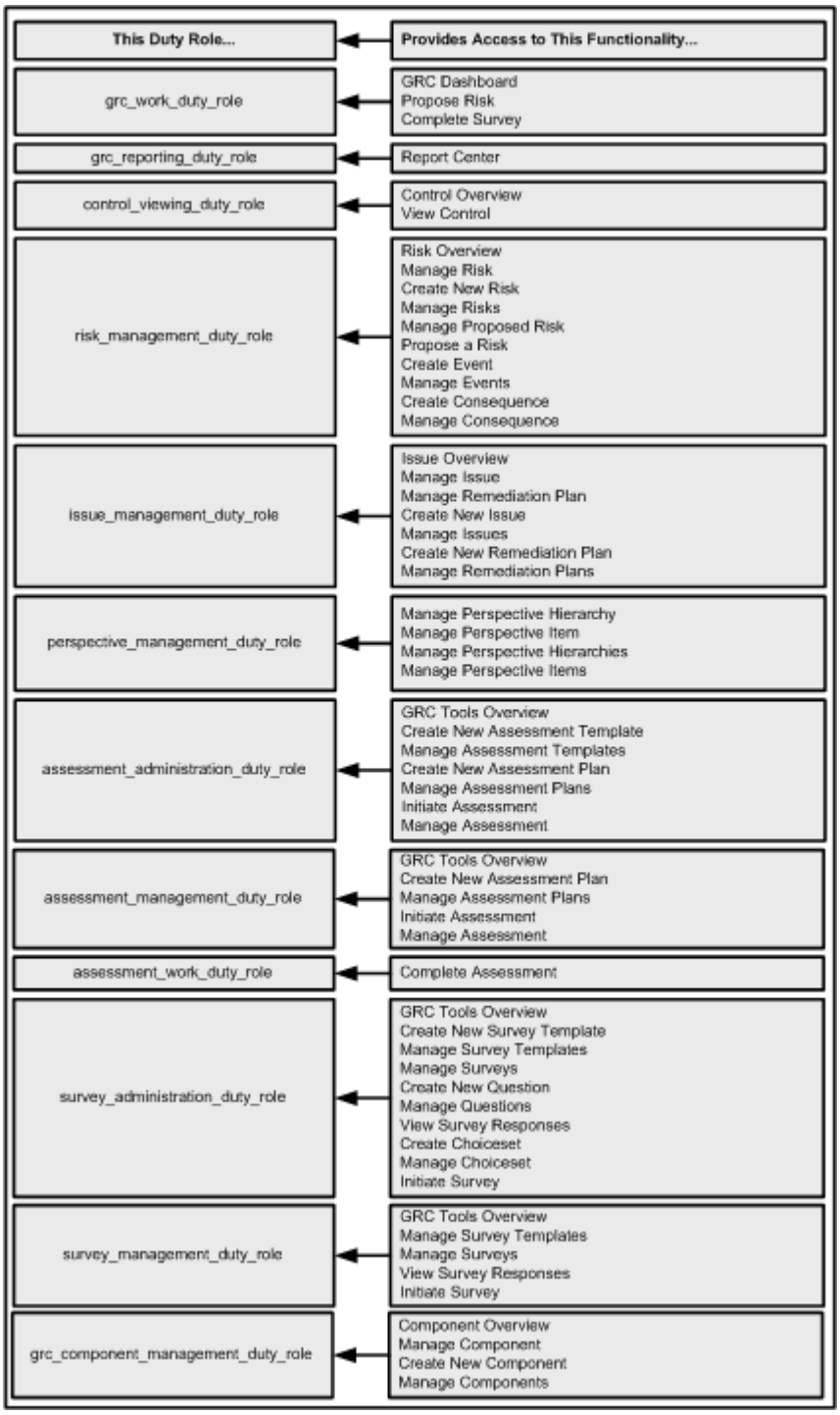
  Duty Roles:



- **Risk Manager**

  Job Role Code: Risk_Manager_Job_Role

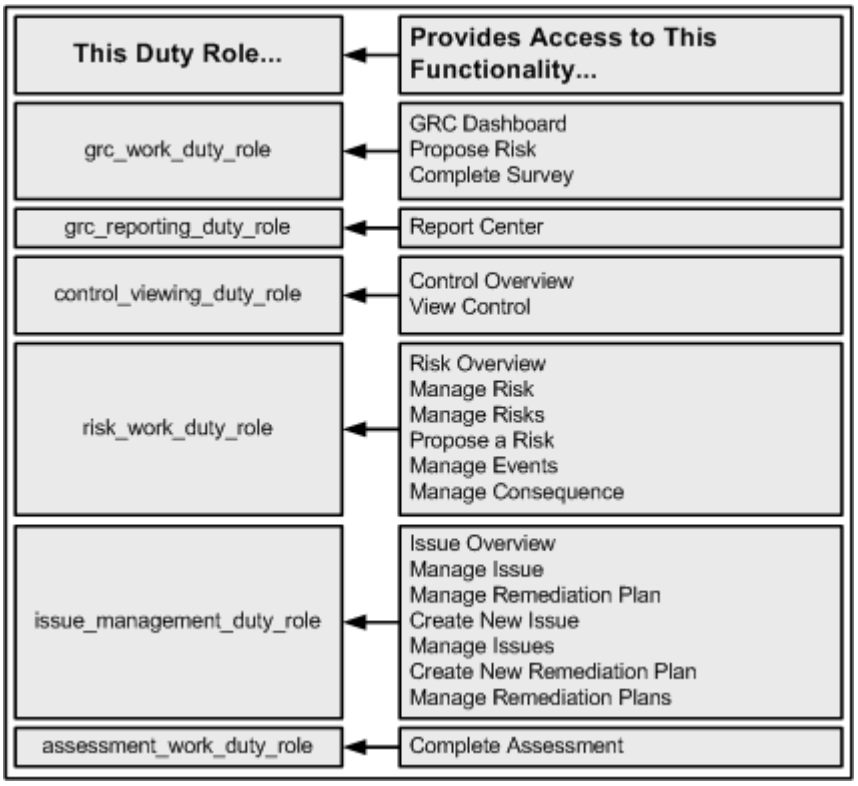
Duty Roles:



- **Risk User**

  Job Role Code: Risk_User_Job_Role

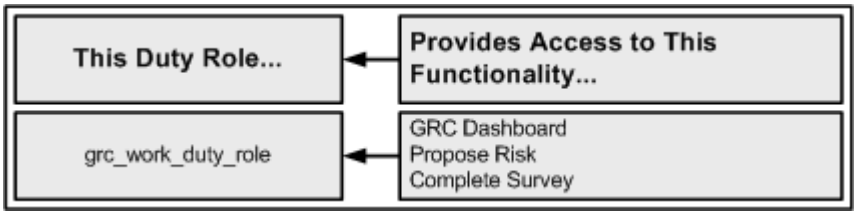
Duty Roles:



- **GRC User**

  Job Role Code: GRC_User_Job_Role

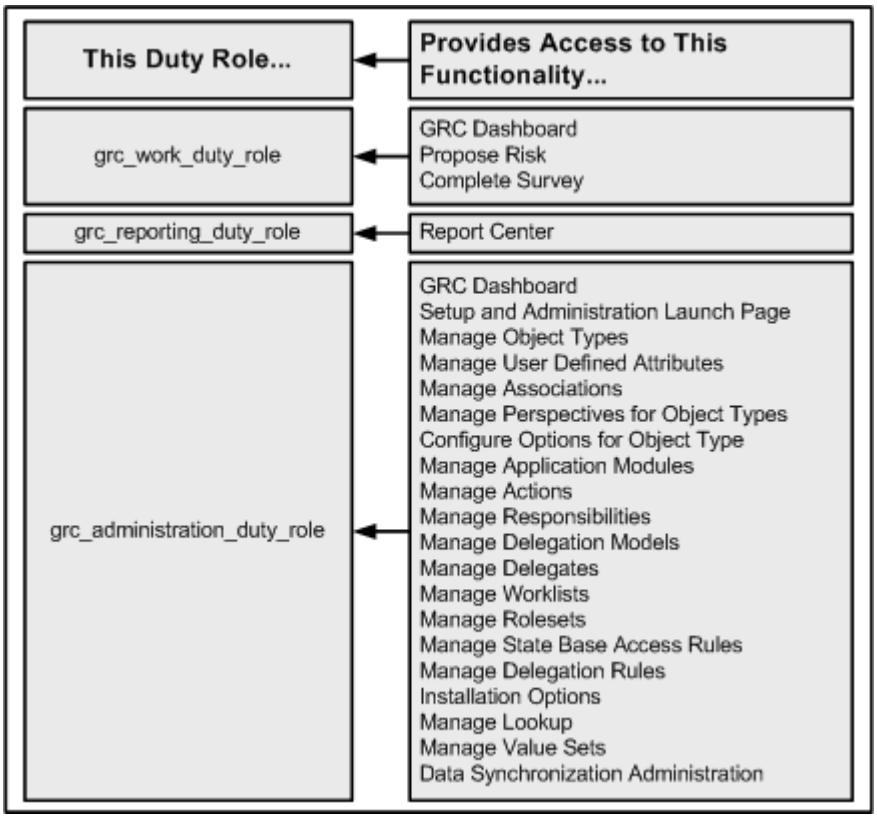
  Duty Roles:



- **GRC Administrator**

  Job Role Code: GRC_Administrator_Job_Role

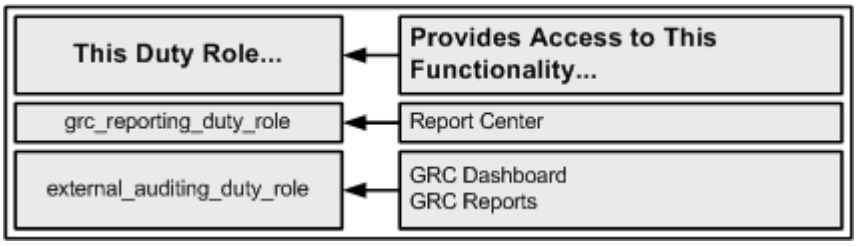
  Duty Roles:



- **External Auditor**

  Job Role Code: External_Auditor_Job_Role

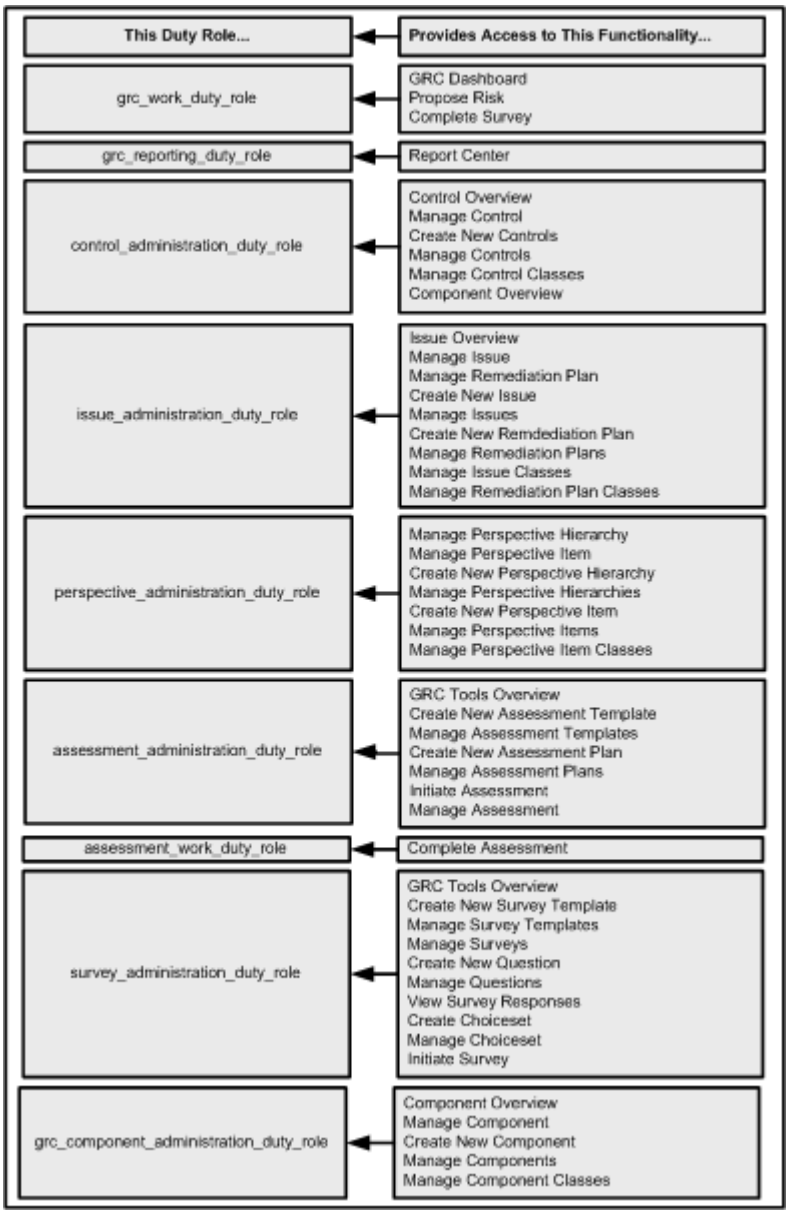
  Duty Roles:



- **Internal Audit Administrator**

  Job Role Code: Internal_Audit_Administrator_Job_Role

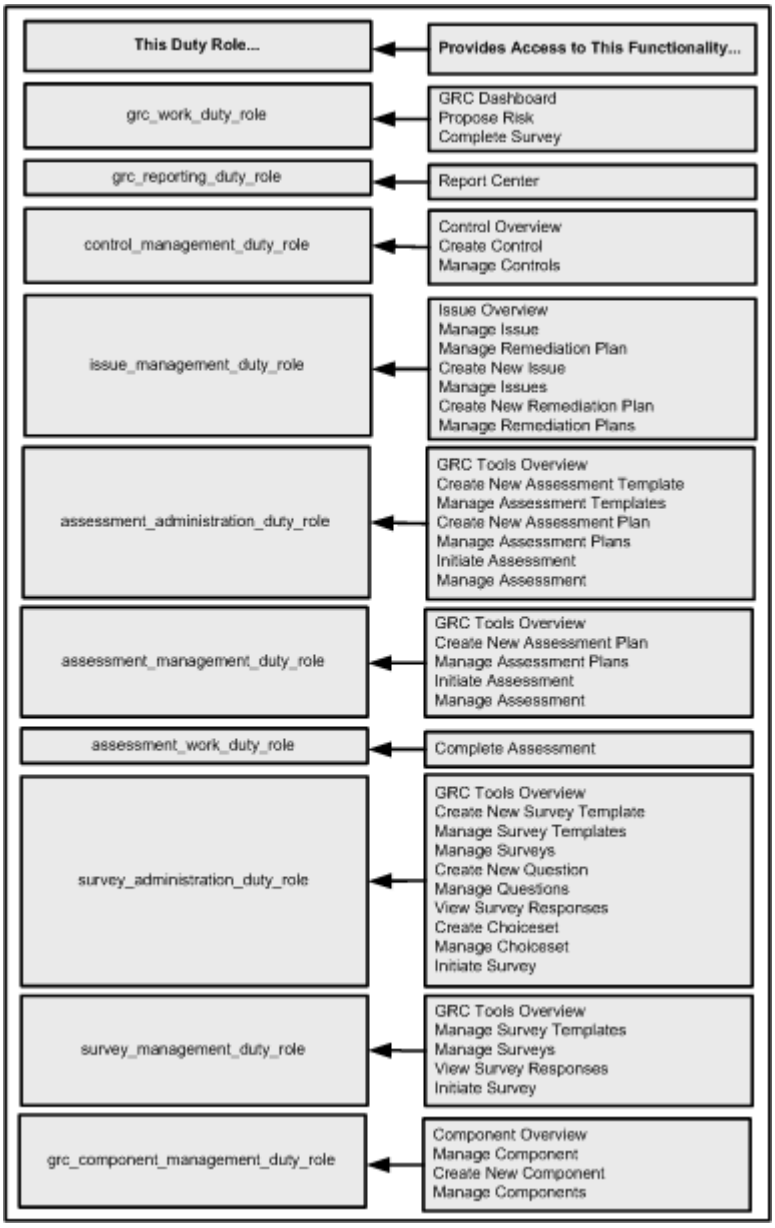
  Duty Roles:



- **Internal Audit Manager**

  Job Role Code: Internal_Audit_Manager_Job_Role

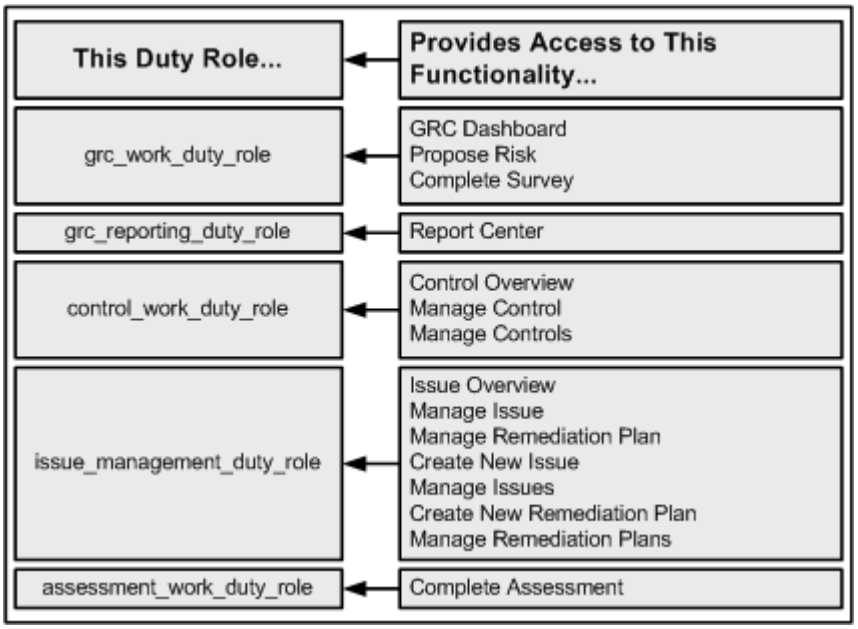
  Duty Roles:



- **Internal Auditor**

  Job Role Code: Internal_Auditor_Job_Role

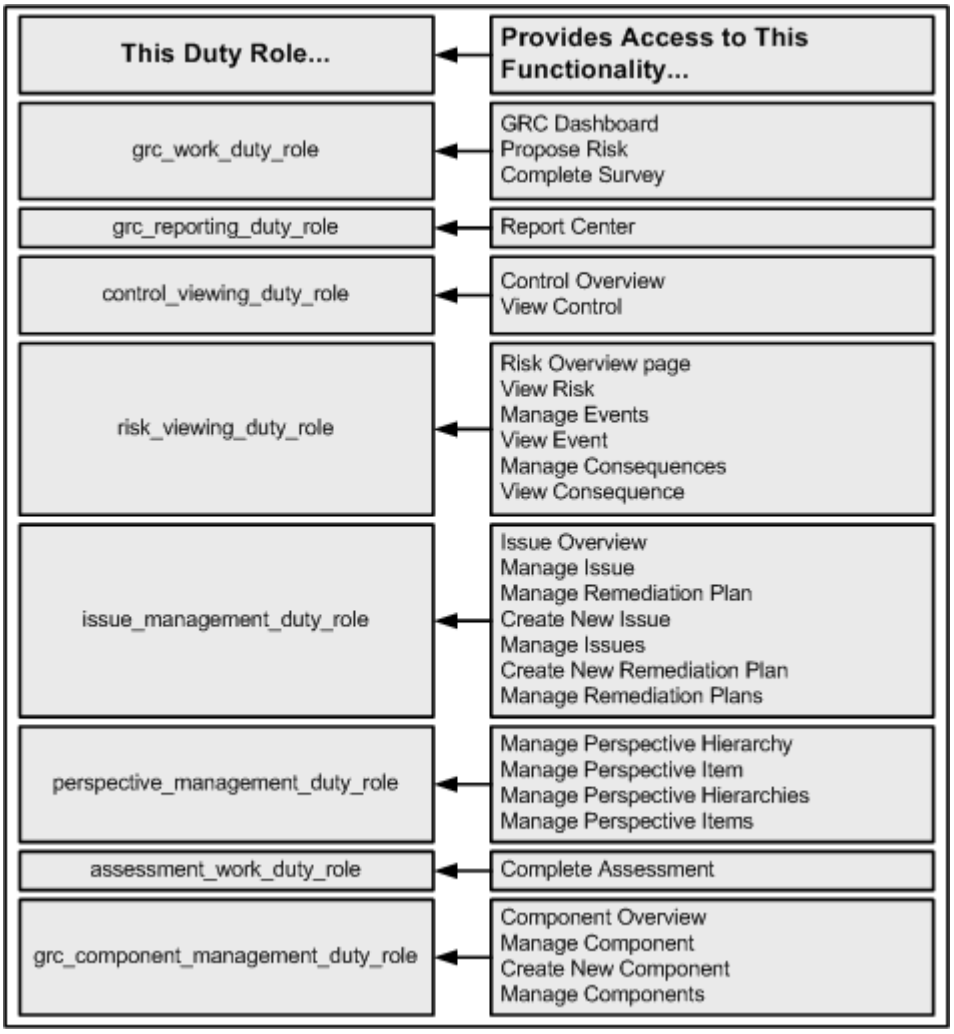
  Duty Roles:



- **Line of Business Manager**

  Job Role Code: Line_of_Business_Manager_Job_Role

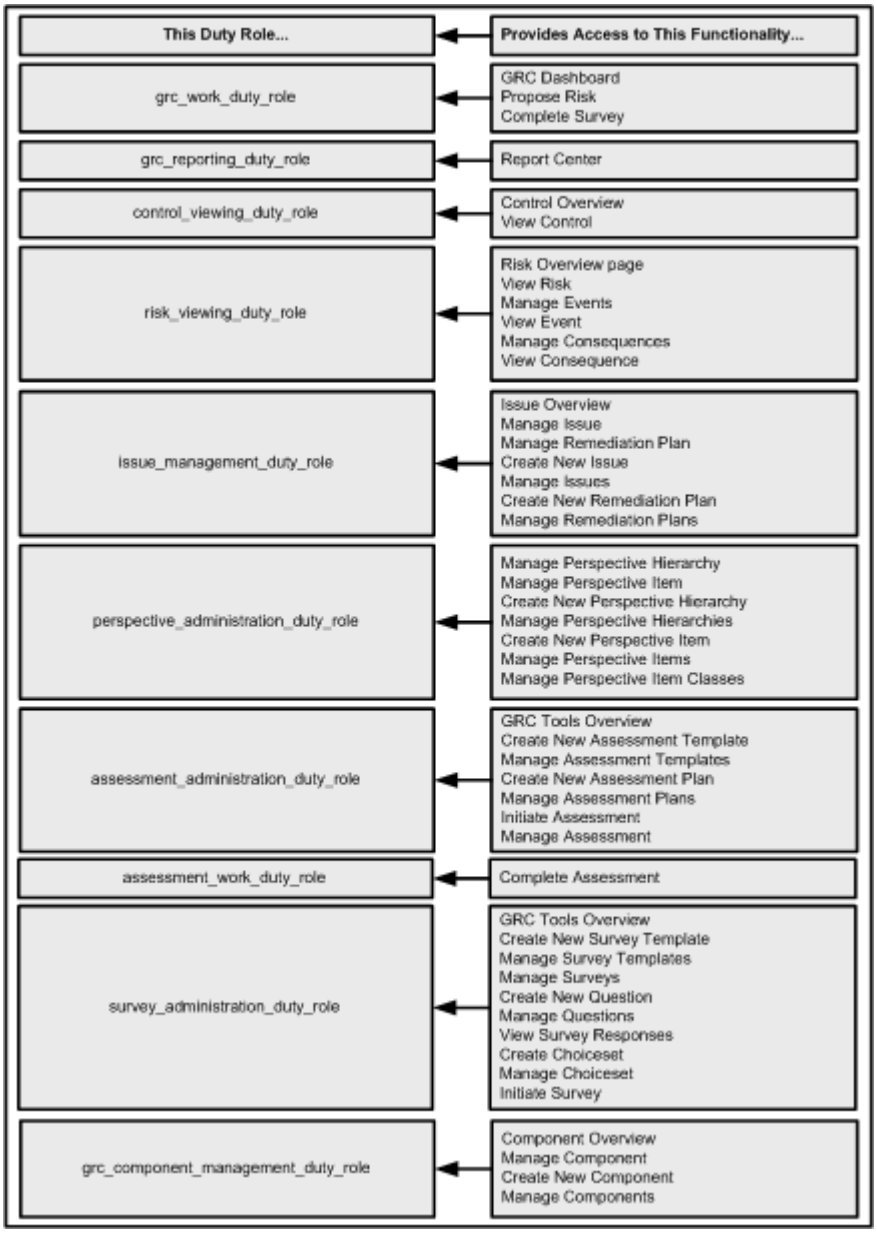
  Duty Roles:



- **Process Administrator**

  Job Role Code: Process_Administrator_Job_Role

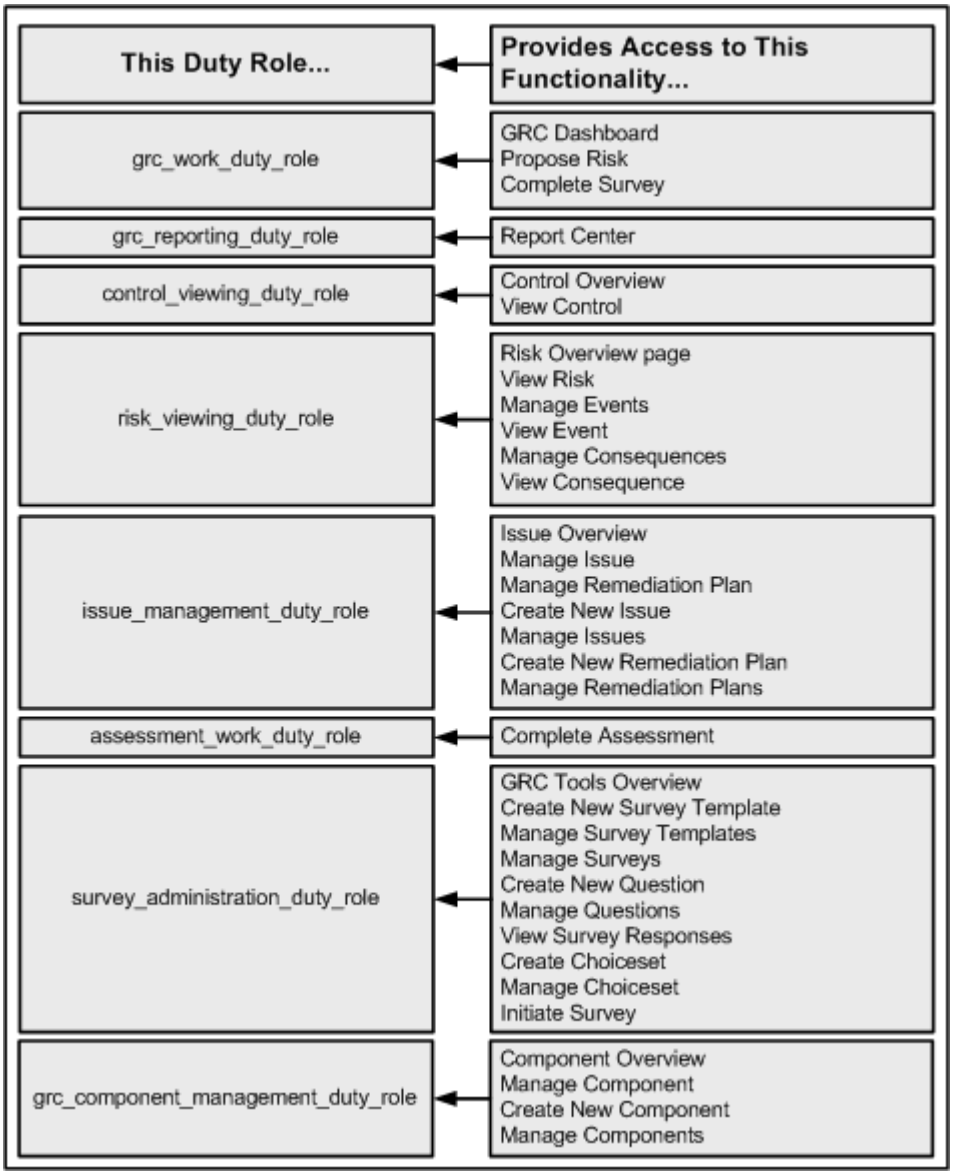
  Duty Roles:



- **Process Manager**

  Job Role Code: Process_Manager_Job_Role

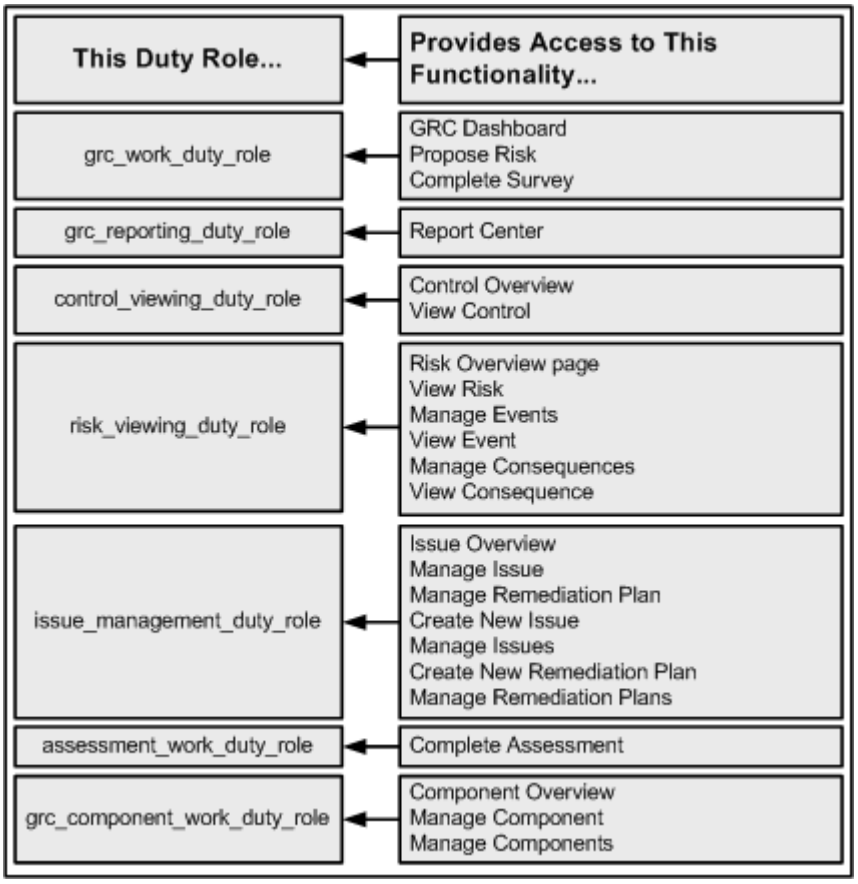
  Duty Roles:



- **Process User**

  Job Role Code: Process_User_Job_Role

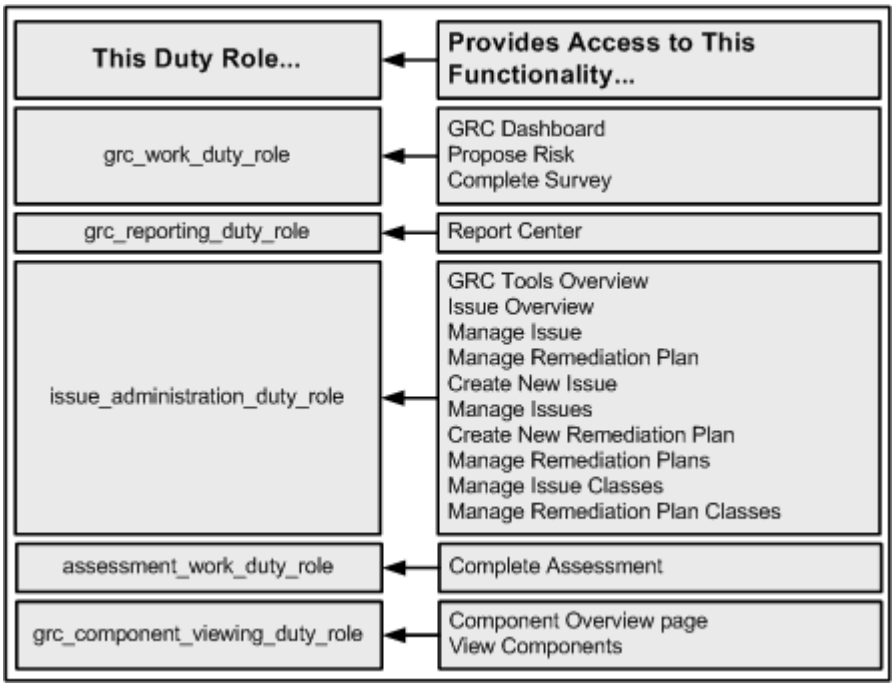
  Duty Roles:



- **Issue Administrator**

  Job Role Code: Issue_Administrator_Job_Role

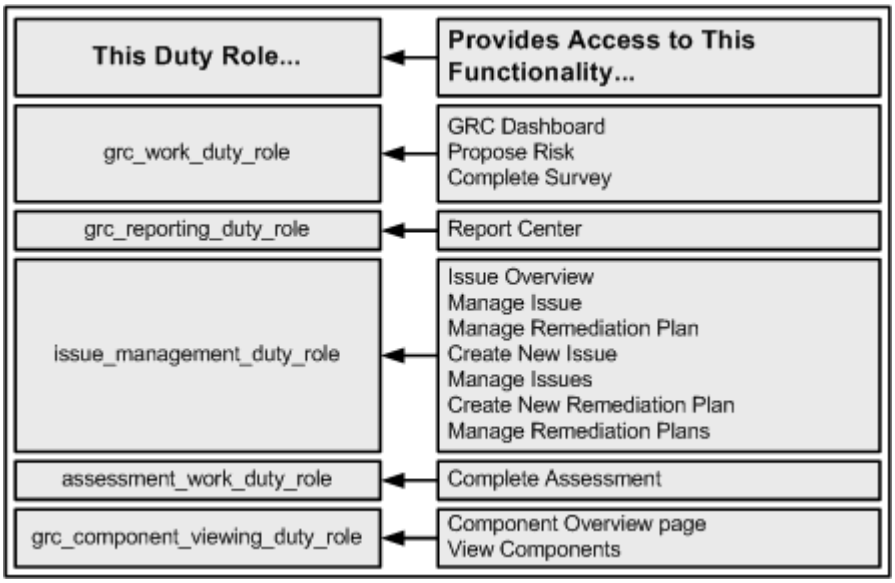
  Duty Roles:



- **Issue Manager**

  Job Role Code: Issue_Manager_Job_Role

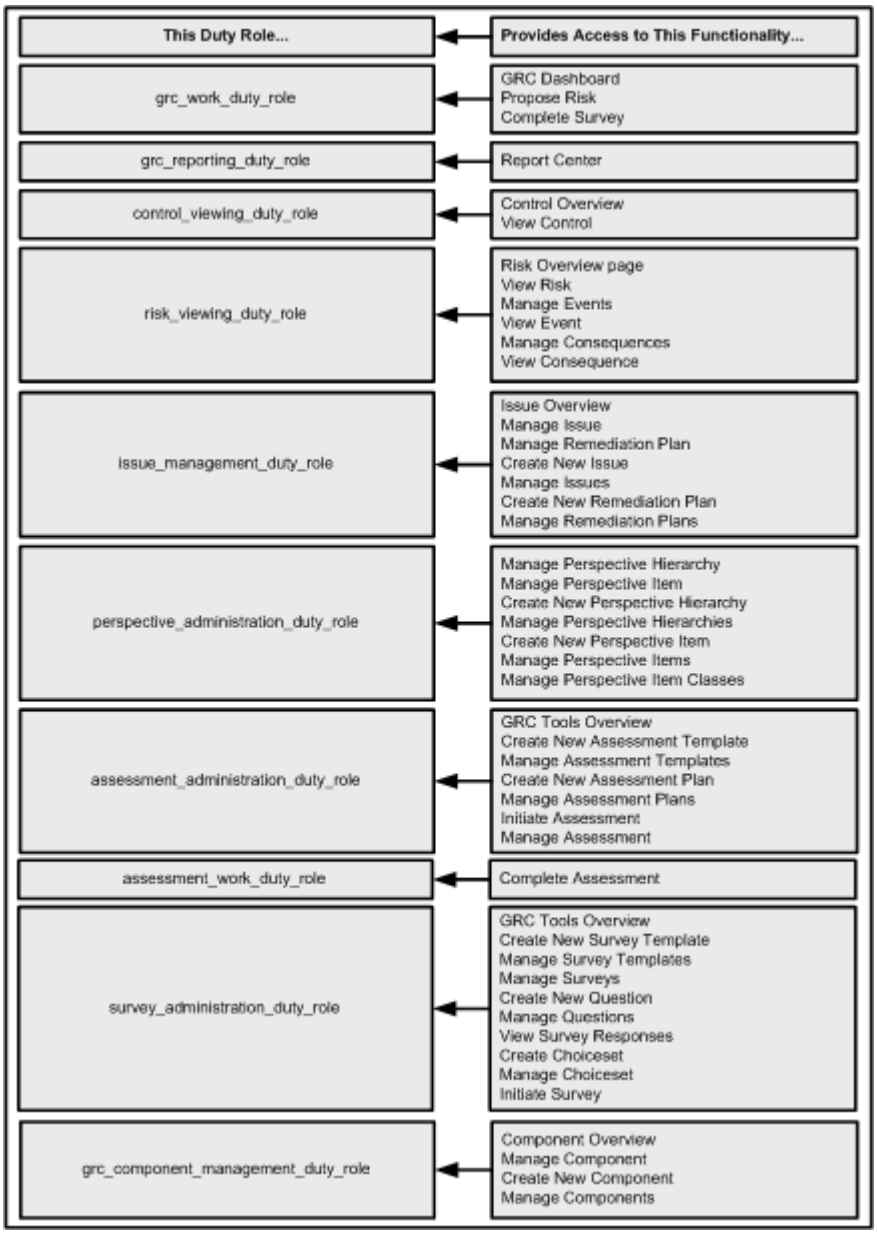
  Duty Roles:



- **Perspective Administrator**

  Job Role Code: Perspective_Administrator_Job_Role

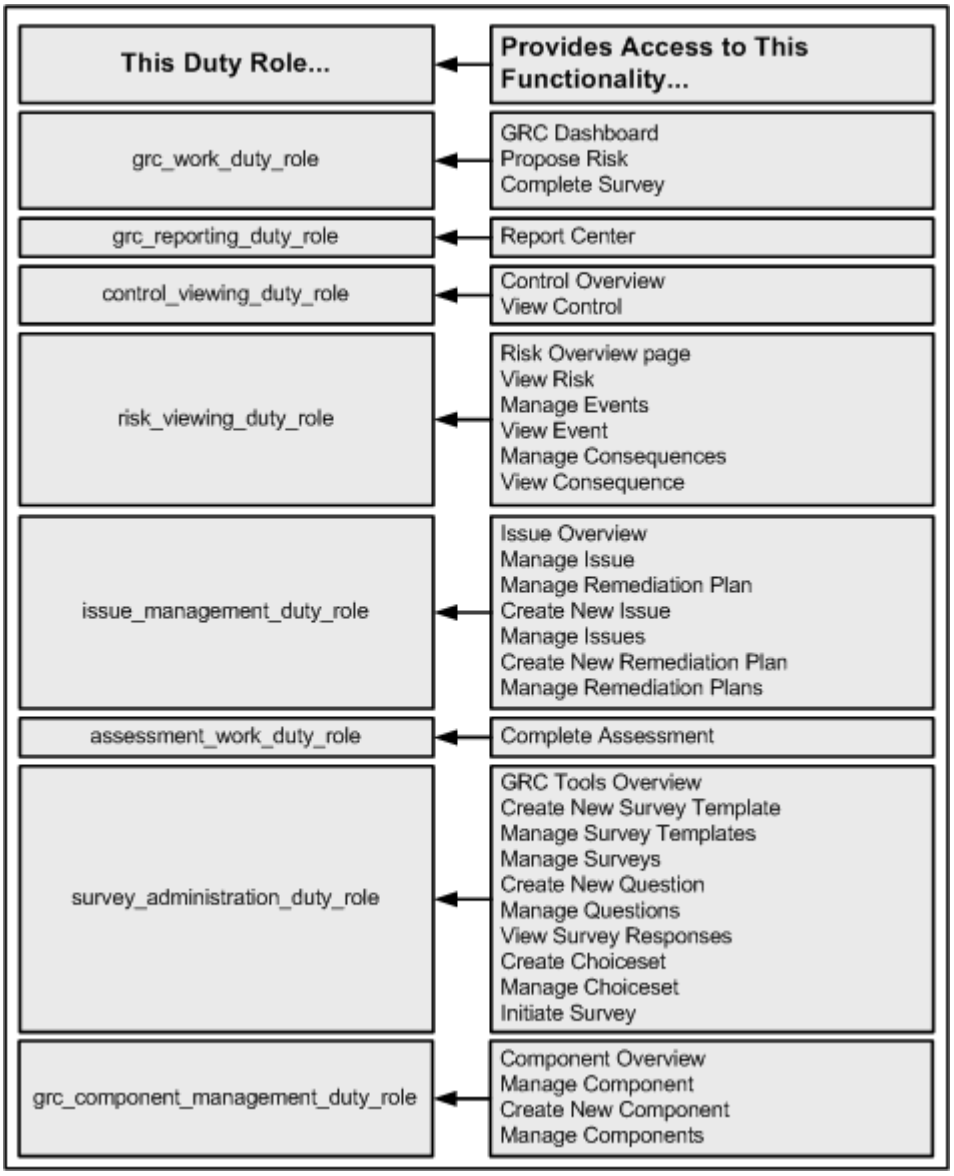
Duty Roles:



- **Perspective Manager**

  Job Role Code: Perspective_Manager_Job_Role

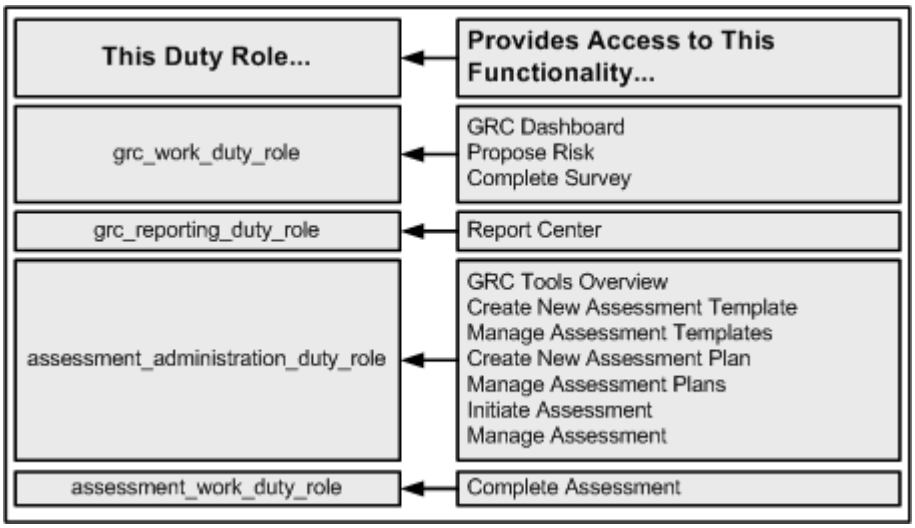
  Duty Roles:



- **Assessment Administrator**

  Job Role Code: Assessment_Administrator_Job_Role

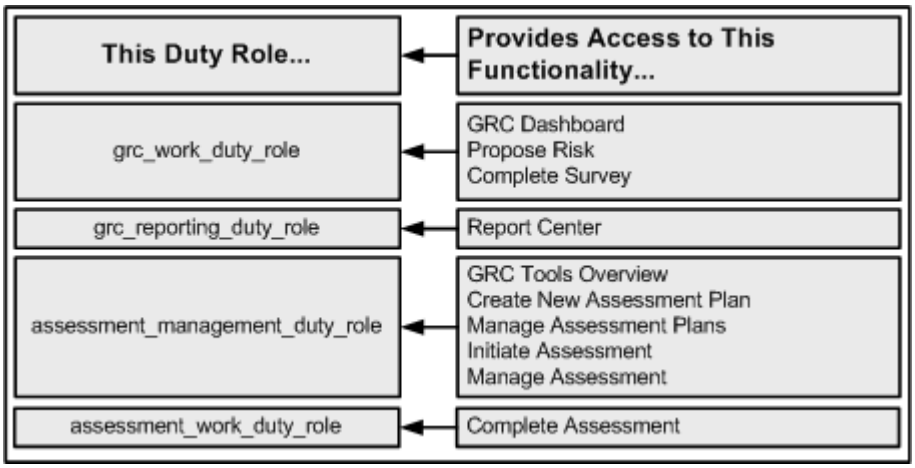
  Duty Roles:



- **Assessment Manager**

  Job Role Code: Assessment_Manager_Job_Role

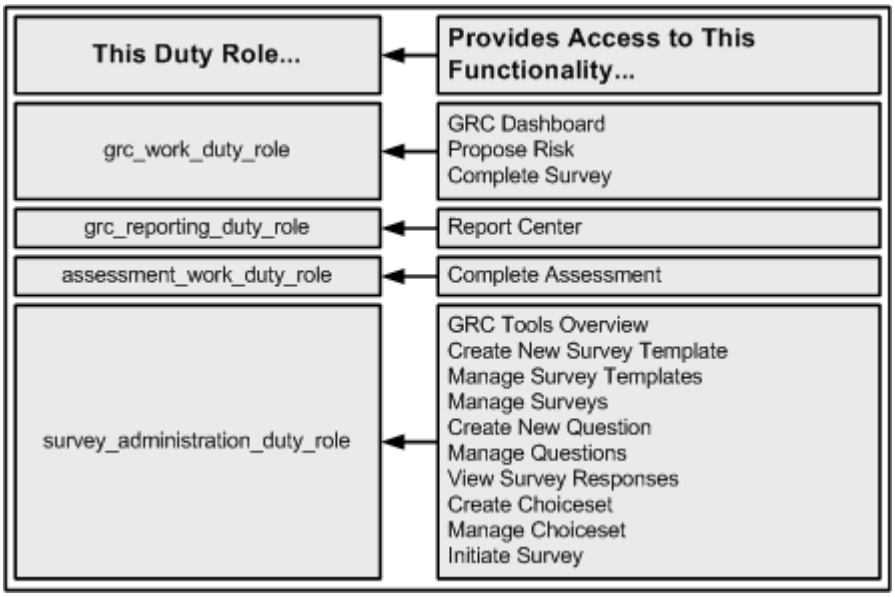
  Duty Roles:



- **Survey Administrator**

  Job Role Code: Survey_Administrator_Job_Role

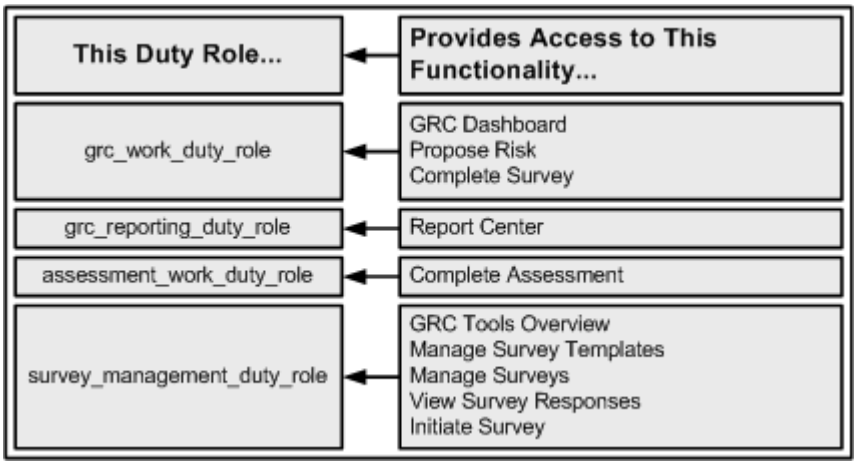
  Duty Roles:



- **Survey Manager**

  Job Role Code: Survey_Manager_Job_Role

  Duty Roles:



Role Creation

To create roles:

1. Login to Enterprise Manager 11g.
2. Select the appropriate WebLogic Domain.
3. From the WebLogic Domain menu, choose Security > Application roles.

4. Select the appropriate Application and Role names.
5. Click the Create button.
6. Enter a name for the new role, and optionally a Display Name and Description.
7. Click the Add Role (+) Icon.
8. Specify if the Role Type is a Group or Application.
9. Click the Search icon to see available roles.
10. Select the roles you wish to add and click the Move icon.
11. Click the Add Users (+) Icon.
12. Click the Search icon to see available users.
13. Select the users you wish to add and click the Move icon.

Refer to the Enterprise Manager online help for additional details.

Enabling Access to Information on Dashboards for Newly Created Roles

Regions on dashboards are displayed based on the role selected on the role switcher. The role switcher is populated based on job roles for the user. For a given job role, the regions on the dashboard are rendered in default position. The seed data for this information is stored in a role to graphic mapping table. When you create a new role, you must insert rows into this graphic table for the new roles, using the appropriate sql commands.

In all of the following commands:

- NewJobRoleName is the job role code
- DefaultorNot? is either 'Y 'or 'N'

SQL Commands Required for Assessment Status Overview Region

```
INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '1',
'GRC_CONTROL_ASMT_ST_OVERVIEW', 'DefaultorNot?');

INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '3',
'GRC_CONTROL_ASMT_ST_OVERVIEW', 'DefaultorNot?');

INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '4',
'GRC_CONTROL_ASMT_ST_OVERVIEW', 'DefaultorNot?');
```

SQL Command Required for Assessment Status Region

```
INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '2',
'GRC_FINCOMP_ASMT_STATUS_GBIE', 'DefaultorNot?');
```

SQL Commands Required for Control Count By Class Region

```
INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '1',
'GRC_CONTROL_COUNT_BY_CLASS', 'DefaultorNot?');

INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '3',
'GRC_CONTROL_COUNT_BY_CLASS', 'DefaultorNot?');

INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '4',
'GRC_CONTROL_COUNT_BY_CLASS', 'DefaultorNot?');
```

SQL Commands Required for Control Count By Type Region

```
INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '1',
'GRC_CONTROL_COUNT_BY_TYPE', 'DefaultorNot?');

INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '3',
'GRC_CONTROL_COUNT_BY_TYPE', 'DefaultorNot?');

INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '4',
'GRC_CONTROL_COUNT_BY_TYPE', 'DefaultorNot?');
```

SQL Commands Required for Control Trend By Costs Region

```
INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '1',
'GRC_CONTROL_COSTS_BY_METHOD', 'DefaultorNot?');

INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '3',
'GRC_CONTROL_COSTS_BY_METHOD', 'DefaultorNot?');

INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '4',
'GRC_CONTROL_COSTS_BY_METHOD', 'DefaultorNot?');
```

SQL Commands Required for Control Trend By Count Region

```
INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '1',
'GRC_CONTROL_COUNT_BY_METHOD', 'DefaultorNot?');

INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '3',
'GRC_CONTROL_COUNT_BY_METHOD', 'DefaultorNot?');

INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '4',
'GRC_CONTROL_COUNT_BY_METHOD', 'DefaultorNot?');
```

SQL Commands Required for GRC Component: Action Item Status Region

```
INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
```

```
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '1',
'GRC_ACTION_ITEM_STATUS', 'DefaultorNot?');

INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '3',
'GRC_ACTION_ITEM_STATUS', 'DefaultorNot?');

INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '4',
'GRC_ACTION_ITEM_STATUS', 'DefaultorNot?');
```

SQL Commands Required for GRC Component: Issue Status Region

```
INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '1',
'GRC_ISSUE_STATUS_BY_COMPONENT', 'DefaultorNot?');

INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '3',
'GRC_ISSUE_STATUS_BY_COMPONENT', 'DefaultorNot?');

INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '4',
'GRC_ISSUE_STATUS_BY_COMPONENT', 'DefaultorNot?');
```

SQL Commands Required for GRC Component: OverDue Assessment Activity Region

```
INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '1',
'GRC_COMPONENT_OVERDUE_ASMT', 'DefaultorNot?');

INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '3',
'GRC_COMPONENT_OVERDUE_ASMT', 'DefaultorNot?');

INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '4',
'GRC_COMPONENT_OVERDUE_ASMT', 'DefaultorNot?');
```

SQL Commands Required for Issue Overview Region

```
INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '1',
'GRC_ISSUE_SEVERITY_DASHBOARD', 'DefaultorNot?');

INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '3',
'GRC_ISSUE_SEVERITY_DASHBOARD', 'DefaultorNot?');

INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '4',
'GRC_ISSUE_SEVERITY_DASHBOARD', 'DefaultorNot?');
```

SQL Commands Required for Open Issues By Business Entity Region

```
INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '1',
'GRC_OPEN_ISSUES_BY_ENTITY', 'DefaultorNot?');

INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '3',
```

```
'GRC_OPEN_ISSUES_BY_ENTITY', 'DefaultorNot?');

INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '4',
'GRC_OPEN_ISSUES_BY_ENTITY', 'DefaultorNot?');
```

SQL Commands Required for Open Issues By Severity Region

```
INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '1',
'GRC_OPEN_ISSUES_BY_SEVERITY', 'DefaultorNot?');

INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '3',
'GRC_OPEN_ISSUES_BY_SEVERITY', 'DefaultorNot?');

INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '4',
'GRC_OPEN_ISSUES_BY_SEVERITY', 'DefaultorNot?');
```

SQL Command Required for Issue Overview Region

```
INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '2',
'GRC_ISSUE_SEVERITY_DASHBOARD2', 'DefaultorNot?');
```

SQL Commands Required for Over Due Remediation Plans Region

```
INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '1',
'GRC_REMED_PLANS_DAYS_OVERDUE', 'DefaultorNot?');

INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '3',
'GRC_REMED_PLANS_DAYS_OVERDUE', 'DefaultorNot?');

INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '4',
'GRC_REMED_PLANS_DAYS_OVERDUE', 'DefaultorNot?');
```

SQL Commands Required for Remediation Plans Percent Complete Region

```
INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '1',
'GRC_REMED_PLANS_PCT_COMPLETE', 'DefaultorNot?');

INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '3',
'GRC_REMED_PLANS_PCT_COMPLETE', 'DefaultorNot?');

INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '4',
'GRC_REMED_PLANS_PCT_COMPLETE', 'DefaultorNot?');
```

SQL Commands Required for Risk Count By Class Region

```
INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '1',
'GRC_RISK_COUNT_BY_CLASS', 'DefaultorNot?');

INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '3',
'GRC_RISK_COUNT_BY_CLASS', 'DefaultorNot?');
```

```
INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '4',
'GRC_RISK_COUNT_BY_CLASS', 'DefaultorNot?');
```

SQL Commands Required for Risk Count By Risk Context Region

```
INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '1',
'GRC_RISK_COUNT_BY_CONTEXT', 'DefaultorNot?');

INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '3',
'GRC_RISK_COUNT_BY_CONTEXT', 'DefaultorNot?');

INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '4',
'GRC_RISK_COUNT_BY_CONTEXT', 'DefaultorNot?');
```

SQL Commands Required for Risk Count By Tolerance Region

```
INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '1',
'GRC_RISK_COUNT_BY_TOLERANCE', 'DefaultorNot?');

INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '2',
'GRC_RISK_COUNT_BY_TOLERANCE', 'DefaultorNot?');

INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '4',
'GRC_RISK_COUNT_BY_TOLERANCE', 'DefaultorNot?');
```

SQL Commands Required for Risk Tolerance By Context Region

```
INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '1',
'GRC_RISK_HEATMAP_BY_CONTEXT', 'DefaultorNot?');

INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '3',
'GRC_RISK_HEATMAP_BY_CONTEXT', 'DefaultorNot?');

INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '4',
'GRC_RISK_HEATMAP_BY_CONTEXT', 'DefaultorNot?');
```

SQL Command Required for Risk Overview By Context Region

```
INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '2',
'GRC_RISK_OVERVIEW_BY_CONTEXT', 'DefaultorNot?');
```

SQL Command Required for Guidance for Propose Risk Region

```
INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '2',
'GRC_PROPOSE_RISK_GUIDE_TEXT', 'DefaultorNot?');
```

SQL Command Required for Compliance Status Region

```
INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '2',
```

```
'GRC_COMPLIANCE_STATUS', 'DefaultorNot?');
```

SQL Command Required for Guidance for Complete Survey Region

```
INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '2',
'GRC_SURVEY_GUIDE_TEXT', 'DefaultorNot?');
```

SQL Command Required for QuickView Region

```
INSERT INTO GRC_DASHBOARD_GRAPH_XREF (ROLENAME, REGION_CODE,
GRAPH_PAGE_CODE, DEFAULT_GRAPH) VALUES ('NewJobRoleName', '5',
'GRC_QUICKVIEW', 'DefaultorNot?');
```

5

Setup and Administration

Configurable Objects Explained

You can configure some objects that are delivered with the product for:

- UDT: User defined object types (UDTs) are used to change the characteristics of base business objects, behavior and relationships to other objects.
- UDA: User defined attributes (UDAs) are used to provide additional attributes to both user-defined and base objects.
- Dynamic Associations: Associations are used to form relationships between business components to support multiple combinations or configurations of objects within application modules.
- Perspectives: Specifies whether or not associations with perspectives can be added or deleted, and whether or not they are required.
- Hide and Hide and Default: Hiding provides the ability to configure a simpler model by allowing select pieces of a model to be hidden.
- Assessment Activities: Identifies which assessment activities you want to include for the specific UDT.
- Delegation: Provides a configurable workflow routing model based on templates and responsibilities.
- State-based Rules: Allows you to control access to business components based on the current state of the component and the user's responsibility

Refer to the rest of this chapter for specific configuration details. Refer to the following configuration tables for details of what each object type can be configured for.

Configuration Table for UDTs, UDAs, Dynamic Associations and Perspectives

Object Type	UDT	UDA	Dynamic Associations	Perspectives
Proposed Risk	Yes	Yes	No	No
Risk	Yes	Yes	Yes	Yes
Risk Treatment Plan	No	Yes	No	No
Risk Treatment	No	Yes	No	No
Risk Analysis	No	Yes	No	No
Risk Evaluation	No	Yes	No	No
Risk Analysis Model	No	Yes	No	No
Risk Evaluation Model	No	Yes	No	No
Risk Assessment Activity	No	Yes	No	No
Event	Yes	Yes	No	No
Consequence	Yes	Yes	No	No
Control	Yes	Yes	Yes	Yes
Test Plan	No	Yes	No	No
Automated Test Instruction	No	Yes	No	No
Manual Test Instructions	No	Yes	No	No
Control Assessment Activity	No	Yes	No	No
Control Assessment Test Plan	No	Yes	No	No
Control Assessment Test Instruction	No	Yes	No	No
GRC Component	Yes	Yes	Yes	Yes
GRC Component Action Item	No	Yes	No	No

GRC Component Assessment Activity	No	Yes	No	No
Perspective Hierarchy	No	Yes	No	No
Perspective Item	Yes	Yes	No	No
Perspective Item Assessment Activity	No	Yes	No	No
Issue	Yes	Yes	No	No
Remediation Plan	Yes	Yes	No	No
Remediation Tasks	No	Yes	No	No
Assessment Templates	No	No	No	No
Assessment Plans	No	No	No	No
Survey Templates	No	Yes	No	No

Configuration Table for Hide and Assessment Activities

Object Type	Configurable Show, Hide, Hide and Default options	Configurable Assessment Activities
Proposed Risk	No	No
Risk	Yes	Yes
Risk Treatment Plan	No	No
Risk Treatment	No	No
Risk Analysis	No	No
Risk Evaluation	No	No
Risk Analysis Model	No	No

Risk Evaluation Model	No	No
Risk Assessment Activity	No	No
Event	Yes	No
Consequence	No	No
Control	No	Yes
Test Plan	No	No
Automated Test Instruction	No	No
Manual Test Instructions	No	No
Control Assessment Activity	No	No
Control Assessment Test Plan	No	No
Control Assessment Test Instruction	No	No
GRC Component	No	Yes
GRC Component Action Items	No	No
GRC Component Assessment Activity	No	No
Perspective Hierarchy	No	No
Perspective Item	No	Yes
Perspective Item Assessment Activity	No	No
Issue	No	No
Remediation Plan	No	No
Remediation Tasks	No	No
Assessment Templates	No	No

Assessment Plans	No	No
Survey Templates	No	No

Configuration Table for Delegation and State-based Rules

Object Type	Delegation	State-based Rules
Proposed Risk	Yes	Yes
Risk	Yes	Yes
Treatment Plan	No	No
Treatment	No	No
Risk Analysis	No	No
Risk Evaluation	No	No
Risk Analysis Model	No	No
Risk Evaluation Model	No	No
Risk Assessment Activity	No	No
Event	Yes	Yes
Consequence	Yes	Yes
Control	Yes	Yes
Test Plan	No	No
Automated Test Instruction	No	No
Manual Test Instructions	No	No
Control Assessment Activity	No	No
Control Assessment Test Plan	No	No

Control Assessment Test Instruction	No	No
GRC Component	Yes	Yes
GRC Component Action Items	No	No
GRC Component Assessment Activity	No	No
Perspective Hierarchy	Yes	Yes
Perspective Item	Yes	Yes
Perspective Item Assessment Activity	No	No
Issue	Yes	Yes
Remediation Plan	Yes	Yes
Remediation Tasks	No	No
Assessment Templates	Yes	Yes
Assessment Plans	Yes	Yes
Survey Templates	Yes	Yes

Setup and Maintenance: General

Installation Options: Critical Choices

The values set within the installation options affect the entire installation, including all data that is entered into the system. When specifying installation options, consider the following:

- What is the local currency for this installation? Because only one currency is supported throughout the installation, the currency that you select is used whenever monetary amounts are entered.
- What language do you want to use for this installation?
- What likelihood and impact model will be used for proposing a risk for this installation? The impact model contains the criteria for weighing the importance of

the event consequence to the risk in the case the event occurred. The likelihood model contains the description or numeric weight of the probability of frequency to be applied to a risk during analysis. The model that you select will be used for all proposed risks.

- How should e-mail notifications be configured?
  - Specify the time that you want the e-mail notifications sent. If you clear all of the time fields, e-mail notification is turned off.
  - Specify if you want all worklist entries to be included in e-mail notifications. The default setting is Yes, which means that both new and previous assignments will be included in the e-mail notification. The worklist entries in the e-mail are separated into two groups; notifications that were sent in a previous e-mail, and those that are new. A new work list entry is one that has been created since the last time e-mail notifications were sent. When the indicator is No, only new assignments are listed in the e-mail notification.
  - Click the Run Now button to initiate an immediate e-mail notification. In the event that e-mail notifications are not received, refer to Troubleshooting, page 6-2.

    Note: Email addresses for the worklist owners come from the user setup in LDAP. The user who runs or sets up e-mail notifications must be part of the SOA administrators group. This will ensure that the correct privileges to query everyone's worklist entries are available. The notification process is started when the SOA Administrator sets the time for notification and saves the changes.

- Server Details: You must specify a server if you are using the e-mail notification feature. Enter the server URL that you want to use for email recipients to log into the application. The format of the URL should be:

  `http://<server_name>:<port_name>`

- If you are using the optional reporting, you must enter the following report setup information:
  - Reports Server URL: This is the URL for navigation to the report center. Enter your Business Intelligence Publisher web URL here.
  - Scenario Start URL: This is the URL used to invoke the startscen.do servlet, which must be invoked to execute the scenario. You must note this URL during your optional reporting installation. The startscen.do servlet is installed as part of your Metadata Navigator installation.
  - Agent Host: Make sure that an agent is created during the optional reports

installation and it is running. Enter the host name or IP address of the workstation that is hosting the ODI agent.

- Agent Port: IP port of the ODI Agent.
- Master Driver: JDBC driver for the ODI Master Repository.
- Master URL: URL used to reach the ODI Master Repository. For example:
  `jdbc:oracle:thin:@[ip_address]:[port_number]:[sid]`
- Master User: User name for the ODI Master Repository.
- Master Password: Password for the ODI Master Repository. This password must be encoded using the command "agent encode [pass]"
- Work Repository: Code or name of the ODI Work Repository you want to connect to.
- ODI User Name: ODI user name. If not defined, the default is SUPERVISOR.
- ODI Password: This password must be encoded by using command "agent encode [pass]"
- Context Code: Code of the context you want to use.
- Log Level: Log level during Scenario execution

Managing Value Sets

You can define values sets that are used when configuring UDAs. When defining a value set, choose a name for the new value set, then specify which lookup type should be used.

> **Note:** The value set type for all UDAs must begin with the prefix "GRC_VALUESET".

Managing Lookup Tables

A lookup table provides a list of values for a specific type of lookup. Lookup tables are associated with various attributes across the EGRCM business components and they support the value sets for a user defined attribute. For example, assessment types, survey types, and reason codes for closing issues all get the list of values presented to the user from a lookup table. You can create a new lookup table to support the value set for a user defined attribute (UDA), update the meaning and description of the delivered lookup tables, and add new values to some delivered lookup tables.

When managing lookup tables, consider the following:

- Which lookup type do you need to update? This is the name of lookup table. Lookup types associated with UDAs must begin with the prefix GRC_VALUESET. You can add new lookup codes to the following lookup types:
  - GRC_SURVEY_QUESTION_TYPE
  - GRC_ISSUE_REASON
  - GRC_REMED_PLAN_PRIORITY
  - GRC_CONTROL_TYPE
  - GRC_ASSESSMENT_TYPE
  - GRC_SURVEY_SURVEY_TYPE
  - GRC_CONTROL_AUDIT
  - GRC_ISSUE_LIKELIHOOD
  - GRC_CTRL_ASSERTIONS
  - GRC_REMED_TASK_PRIORITY
  - GRC_CONTROL_FREQUENCY

    Note: When creating a new lookup type that will be used with a UDA, you must preface it with "GRC_VALUESET".

- What will be the code for the lookup value? This is the value that the user selects from a list of values.
- What is the meaning for the lookup code? This is the descriptive term used for the code. For example, if the code is 1 on a scale of 1 to 5, the meaning of 1 might be "Lowest"
- What is the description for this lookup value?
- At what point in the list of values should this value be displayed?

For example, say that you have created a new UDA called Risk Level, and you need to create the lookup table that contains the list of values for it. You might define the first lookup as follows:

- Type: GRC_VALUESET_RISK_LEVEL

- Code: 1
- Meaning: Low
- Description: Low risk level
- Sequence: 1

Managing Application Modules

An application module is a collection of component types (risk, controls, etc) that defines the underlying information model of the GRC solution, such as a financial compliance model. Although you cannot create new application modules, you can extend the delivered Financial Governance module.

When managing application modules, consider the following:

- What is the name of the module that you wish to modify?
- Which entity types require updating? Although you cannot change entity types that are seeded in the delivered Financial Compliance module, you can enable new relationships to UDTs.
- Which roles should be able to access this module?

Performing Data Synchronization Administration

Data synchronization is used to populate the reporting database. Configuration for the synchronization is set in the Installation Options Report Setup Information page, page 5-7.

When you first access the Data Synchronization Administration page, no data is displayed. When you click the Refresh button, the most recently run synchronization job details are displayed. Click the Synchronize button to start the process. Once you have initiated the synchronization, you can monitor its progress.

Setup and Maintenance: Object Type Maintenance

Object Type Maintenance Explained

Some system-delivered objects allow you to extend the base characteristics. You can extend these base objects by creating a User-Defined Object (UDT). For a complete list of objects that support UDTs, refer to Configurable Objects Explained, page 5-1. UDTs:

- Leverage business specific metadata

- Inherit the characteristics and behavior of the base object

Managing Object Types: Critical Choices

When creating a new object type, consider the following:

- What is the parent (or base) object type? For example, Risk, Event, Consequence.
- What name should the new object type be assigned?

Configuration Options Explained

Configuration options for object types are specified at the UDT level and include:

- Configurability Options: Provide the ability to configure a simpler risk model by allowing select pieces of a model to be hidden. You can choose:
    - Hide Option: Controls whether or not the user interacts with events, consequences or treatment plans. If hidden, the user is never exposed to these sub components.
    - Hide Event: Hides the Event region on the Create, Edit and Manage Risk pages. Hide Event implies hiding consequence. Event and consequence are also hidden on the Proposed Risk page. You can choose to hide consequences but not events.
    - Hide Consequence: Events are displayed, but no relationships to consequences are displayed within the Events Region of the Create, Edit and Manage Risk pages.
    - Hide Treatment: Treatment plan, treatment and control stratification are all hidden on the Create, Edit and Manage Risk pages. Risk does not have a relationship to control within Risk Management. You can hide treatment plans, which implies hiding treatments and control stratification. This implies no relationship to controls.
    - Hide and Default: Only applicable for treatments. Hides treatment plans and treatments but exposes related control stratification within the Manage Risk page. The system generates one default treatment plan and treatment in order to store the control stratification information.
- Assessment Activity Definition: Identifies which assessment activities you want to include for the specific UDT. You can also enter additional guidance text for assessment activities by UDT.

Managing Configuration Options for Object Types: Critical Choices

When managing configuration options for object types, consider the following:

- Which features should be available to which users?
- Which assessment activities should be enabled or disabled? Assessment activities include Design, Operating, Audit Test, Certify and Documentation Update.
- What information about this object might the user need to know while performing the assessment activity? For example, if you created a new object type of Financial Governance Process, for guidance text you might enter "Process Design Assessment enables the reviewer to determine if the control environment for the particular process is designed effectively to mitigate the process risks."

Managing Perspectives for Object Types Explained

When you manage perspectives for object types, you add and or delete associations with perspectives, and specify whether or not they are required. This allows you to further extend the definition of business processes by relating perspectives to object types.

Base perspectives are the foundation for defining custom perspectives that can be created for a process at both the base and UDT level. Establishing a perspective for a base object makes that perspective available for all types (UDTs) of that base object. Perspectives at the UDT level are in effect for just that specific user defined type. Perspectives are dynamically displayed within the UI in the Perspective region of Create, Edit and Manage Perspective pages.

Managing Associations

Associations are used to form relationships between business components to support multiple combinations or configurations of objects within application modules. There are various combinations of associations between business components to support different information frameworks needed to support processes or application modules.

Business components can be shared across application modules, but associations between business components vary by business function or focus. Identification of the associations that are appropriate for the business components is performed within the module definition.

When managing associations, consider the following:

- What will the primary type be? For example, risk , control, etc.
- What will the secondary type be? For example, risk , control, etc.

User Defined Attributes for Object Types Explained

You can add additional attributes to both user-defined and base objects such as risks, controls, GRC components, perspectives, issues, survey templates. These additional attributes automatically display on the object Create, Edit and Manage pages in the Additional Information region. When creating a user-defined attribute (UDA) the user has the ability to select properties, such as Data Type and so forth.

UDAs are available on the base object as well as UDTs. Establishing an attribute at the base object makes that attribute available for all types (UDTs) of that base object. Attributes at the UDT level are in effect for just that specific user defined type. Base Objects that do not support UDTs (such as Treatment Plan, Test Plans, Assessment Results) still support UDAs.

When creating a user-defined attribute (UDA) can specify the following properties:

- Data Type (String Translatable, Number, Date, String NonTranslatable)
- Control Type (Text box, Check box, Dropdown)
- Value Set
- Attribute Name
- Order
- Disabled
- Required

For a complete list of objects that support UDAs, refer to Configurable Objects Explained, page 5-1

Are there limits on how many UDAs that I can create for an object?

UDA creation is limited to the following:

Objects with this Data Type...	Can Have this Many UDA Fields...
Numeric	30
Date	30
Non-Translatable String (for example, codes)	40
Translatable String (for example, Department Name)	40

Setup and Maintenance: Delegation

Delegation provides a configurable workflow routing model based on templates and responsibilities. As part of managing delegation setup, you can attach different types of actions to responsibilities. This provides granular security ACL (Access Control Lists) based on responsibilities. Delegation is defined for the base object and applies to all UDTs of that base.

Managing Delegates Explained

Managing delegates allows you to reassign a user or role to another user or role within the current delegation. This provides the capability to perform a mass change to any object that uses that delegation; it replaces the delegate within the individual instances of the business component. When managing tasks, you need to decide to which delegate you want to reassign the selected delegate's tasks. You can refine the list of delegates with the search criteria and replace all or just those selected.

Managing Delegation Models: Critical Choices

A delegation model is the template that identifies the set of responsibilities for a specific object type. This is what you see within component pages to assign user or roles to a specific responsibility. A delegate is an enterprise user defined within the LDAP. Who can be assigned the responsibility is controlled by the Roleset.

The model controls how many reviews or approvals are required before progressing to the next action within the delegation process. You can introduce as many review and approval cycles as needed by adding additional responsibilities and adjusting the order.

When creating a delegate model, consider:

- Responsibility: The responsibility for which you are creating this delegate model such as Reviewer or Approver.
- Order of Action: A numeric value that specifies the order of execution of action associated with the responsibility. This is only valid when there are multiple responsibilities associated to the same action.
- Default To: Select whether the default delegate should be the current user, a specific role, or a roleset.
- Default Value: The default delegates for the responsibility.
- Require Reviewers Approvers: A numeric value that specifies how many users must act before the next action can occur. For example, how many delegates must review a document before it can be put into the approval cycle.
- Security Roleset Code: These Roles restrict the drop down list of possible delegates

at runtime for this Delegation Model.

Managing Responsibilities Explained

Managing responsibilities identifies the individual responsibilities involved with a specific object type and the action to which they are assigned.

When creating responsibilities, consider:

- Code
- What action should the delegate be able to perform? Actions are the BPEL processes. For example, Review BPEL Process, Approve BPEL Process, Notify BPEL Process.
- What is the activity that the delegate should be able to perform? Activities are system defined specific tasks within the delegation for that specific object type. For example, for Risk they are owner, reviewer, approver, analyzer, evaluator, assessor, viewer and administrator. Activities include:
    - Administrator: An Administrator has all the same access as an Owner, but they do not receive notifications for the business entity.
    - Analyzer: (Applicable to Risks only) Responsible for examining a risk to determine the level of risk that is involved.
    - Approver: Responsible for affirming that any changes made to business entities are appropriate or correct.
    - Assessment Approve: Responsible for affirming that information in an assessment is appropriate or correct.
    - Assessment Review: Responsible for examining an assessment that has been performed by an assessor.
    - Assessor: Responsible for completing the assessment activity which includes reviewing how objects are defined and implemented to ensure that the appropriate levels of documentation and control are in place.
    - Assigned To: This activity is not in use.
    - Evaluator: (Applicable to Risks only) Responsible for appraising a risk to determine if treatment or additional treatment is required.
    - Identifier: (Applicable to Proposed Risks and Issues only) This activity is used to track the user that reported a proposed risk or issue. For all other objects, the creator is the owner, but proposed risks and issues are reported and then ownership is assigned to someone else.

- Manage Issue: Responsible for supervising and performing general management for issues.
- Owner: Responsible for administering and maintaining the business entity.
- Remediator: Responsible for administering and maintaining remediation plans.
- Reviewer: Responsible for examining changes made to the business entity.
- Tester: This activity is not in use.
- Translator: (Applicable to surveys only) Responsible for translating survey questions and instructions--Viewer: A viewer can look at but not modify the business entity.

- Should the delegate have read only access?

Managing Worklists Explained

Managing worklists allows you to reassign a worklist to another user or role. It only changes the assignment within the worklist entries. The next time the entity is submitted, the regular delegates are assigned the worklist. This task is specific to administrators; users cannot reassign there own worklist. You can reassign by:

- Entity (object) Type
- Responsibility
- Action
- Delegate
- Any combination of the above

Managing State Based Access Rules Explained

State based access allows you to control access to business components based on the current state of the component and the user's responsibility. State based access is in addition to the user security policy which indicates whether the user is granted access to a business component at all. State based access controls can only remove or limit a privilege that a user has already been granted through their security profile.

Example: State Based Access A risk owner can change a risk that they have created as long as the risk is in the New, Active or Work in Progress state (that is, the risk has not yet been submitted for review and approval.) However, once the risk is in the Review and Approval process, (that is, it is in either In Review or Awaiting Approval status), the risk owner can no longer make changes to the risk.

When managing state based access rules, consider:

- Editing Access to Attributes Rules: Choose the attribute, then specify the access (read only or read write)
- Editing Access to Actions Rules: This allows you to specify the states in which an object can accessed for a specific responsibility.

Managing Actions Explained

The Manage Actions page is where you create actions and then later associate these actions to responsibilities.

Managing Rolesets Explained

Managing rolesets involves defining the set of roles that are appropriate for a particular responsibility. Rolesets are defined for an object and responsibility combination. They control which users and roles can be assigned within the delegation at run-time.

Managing Rolesets: Critical Choices

When managing rolesets, consider the following:

- The Code: This is the unique identifier for the roleset. For example, Risk_Evaluator_Roleset.
- A name for the roleset
- What roles should belong to this role set

Managing Delegation Rules Explained

Managing delegation rules consists of identifying which changes require review, approval or a notification of the change. All changes are tracked and the delegation rule determines which of those changes require review and or approval. Notification involves sending notices to owners of other components that are related to the one that was just change; this is also controlled by the rule. Only exceptions are listed within the rule.

Managing Delegation Rules: Critical Choices

When managing delegation rules, consider:

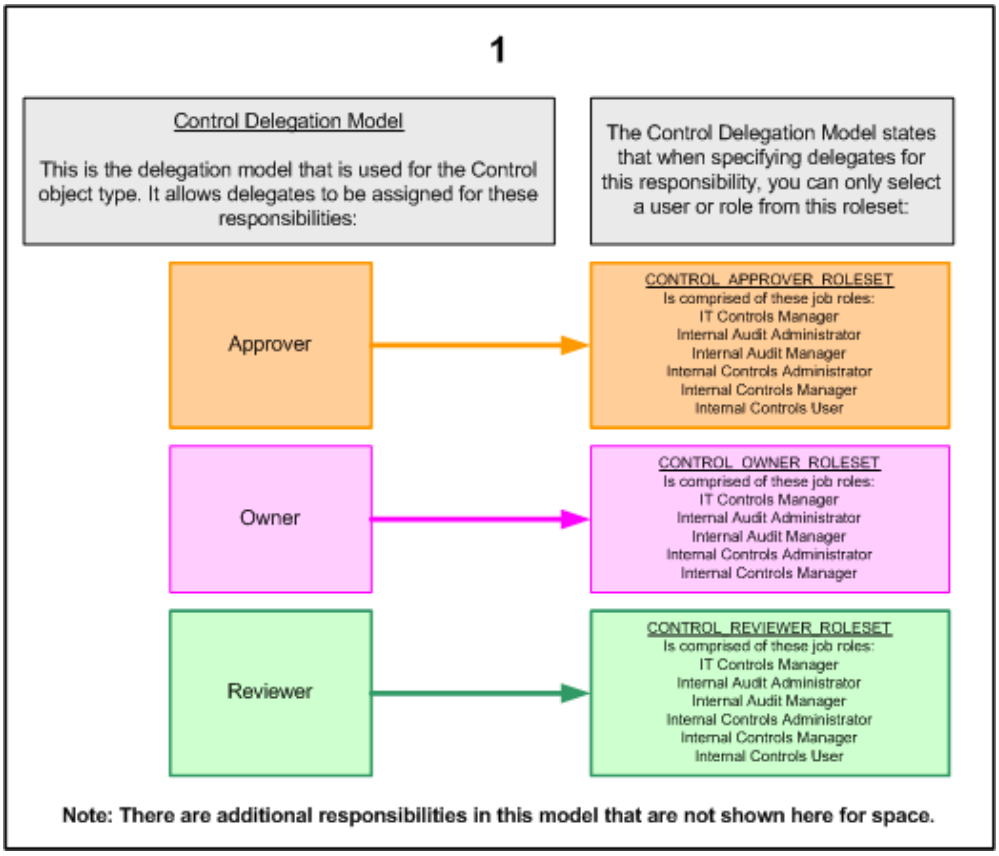
- Attribute Type (Attribute, Association)
- Attribute

- Privileges (Review, Approve, Notify)

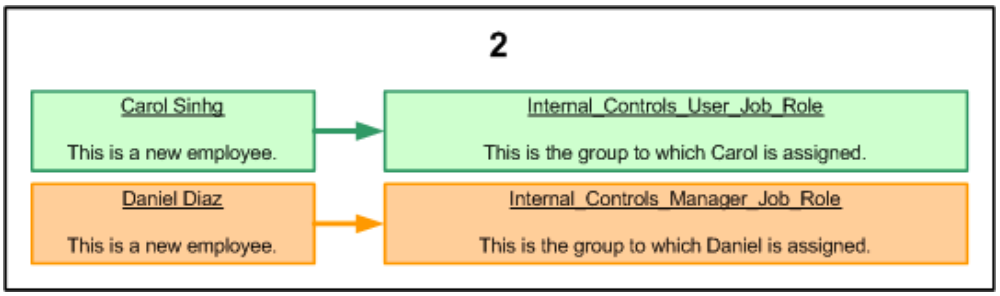
Case Study: Understanding Users and Delegates are Related

This case study shows how delegation uses models, role sets and responsibilities to assign work to an end user:

1. Oracle ships EGRCM with seeded defined objects. The objects have delegation models associated to them as part of their definition. Shown here, for example, is the delegation model for the seeded Control object.



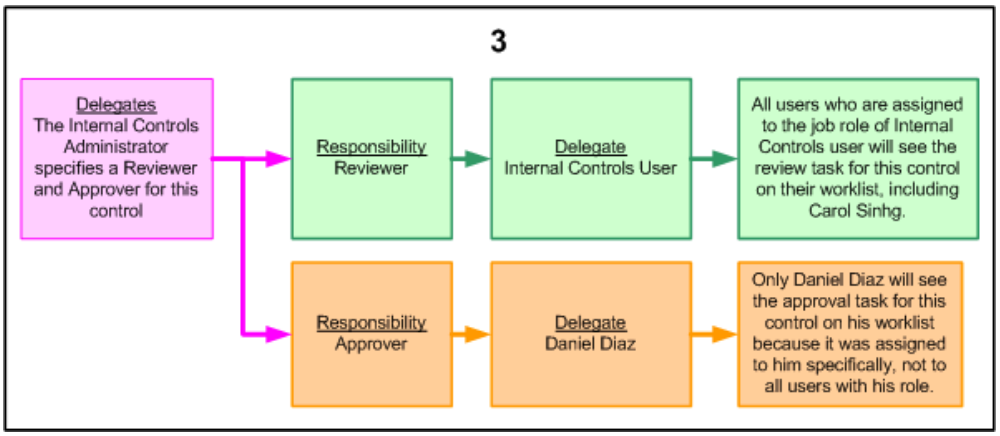
2. Two new users are created by the corporate security administrator. In this example, one of them is assigned the job role of Internal Controls User, and the other is assigned the job role of Internal Controls Manager.



3. A user with the role of Internal Controls Administrator creates a new control. When the Administrator specifies a Reviewer and Approver, the list of values he can choose from comes from the Control Delegate model. As shown here:

   - The reviewer delegate is the role of Internal Controls User. This means that all users who have this role will see this task on their work list

   - The approver delegate is the user Daniel Diaz. He has the Internal Controls Manager role, but this approver task was assigned directly to him, so he is the only user who will see it on his worklist



6

Troubleshooting and Optional Configuration

Tuning

Before you begin, ensure that the OEL 64-bit operating system is running.

Operating System Tuning

Follow this procedure to tune the operating system.

1. Navigate to the directory $MW_HOME/user_projects/domains/base_domain/bin
2. Open the file setSOADomainEnv.sh
3. Make the following changes:
   - PORT_MEM_ARGS="-Xms512m –Xmx2048m"
   - PORT_MEM_ARGS="${PORT_MEM_ARGS} -XX:PermSize=256m -XX:MaxPermSize=1024m"
4. Restart the WebLogic servers.

Database Tuning

1. Login as an Oracle user with sysdba privileges
2. Enter the following commands:

```
SQL> alter system set processes=5000 scope=spfile;
SQL> alter system set sessions=5000 scope=spfile;
SQL> alter system set open_cursors=3000 SCOPE=SPFILE;
```

3. Restart the database.

Troubleshooting

The following tools are available:

- Use the WebLogic Server Console to:
  - Manage system resources such as increasing the connection pool of JDBC DataSource
  - Manage users and Enterprise roles
- Use the Enterprise Management console to:
  - Check the overall health of the system
  - Check the health of the composites
  - Manage application policies
  - Manage OWSM policies
- Use the database console to:
  - Verify if the DB objects were created properly
  - Verify if seeded data was inserted properly
- View the following log files
  - AdminServer Log:
    `$MW_HOME/user_projects/domains/<domain>/servers/AdminServer/logs/AdminServer.log`
  - SOAServer Log:
    `$MW_HOME/user_projects/domains/<domain>/servers/soa_server1/logs/soa_server1.log`
  - GRC Server Log:
    `$MW_HOME/user_projects/domains/<domain>/servers/grc_server1/logs/grc_server1.log`

Troubleshooting E-mail Notifications

If email addresses are not setup or if they are incorrect, errors will appear in the soa_server1-diagnostic-1.log file. If an email is incorrect, you will see following message in the soa_server1-diagnostic-1.log file:

`ORABPEL-31015`

```
Error while sending notification. Error while sending
notification to 'email:username@company.com

Possible causes : SDPMessaging Driver not configured; Invalid To
Address is used; Email server/Messaging gateway is down; using
IP address as part of email IDinstead of domain name;
```

If no email is specified, you will see the following message in the soa_server1-diagnostic-1.log file:

```
ORABPEL-31015

Error while sending notification. Error while sending
notification to 'email:null; 968a49b08c575d4c01bbc11b38342263'

Possible causes : SDPMessaging Driver not configured; Invalid To
Address is used; Email server/Messaging gateway is down; using
IP address as part of email IDinstead of domain name;
```

In either case, check the user setup in LDAP to correct the e-mail address.

Index