Oracle® Enterprise Governance, Risk and Compliance Manager

Implementation Guide

Release 8.6.4

Part No. E26566-01

November 2011

ORACLE

Oracle Enterprise Governance, Risk and Compliance Manager Implementation Guide

Part No. E26566-01

Primary Author: Denise Fairbanks Simpson

Contents

1 Enterprise Governance, Risk and Compliance Setup Overview

Data Types 1-1
Diagnostic Steps 1-2
EGRCM Setup Flowchart 1-4
Setup Checklist 1-4
Administration Setup 1-4
Financial Governance Module Configuration 1-6
Module Management 1-7
Module Object Configuration 1-8
User-Defined Attributes for Objects within a Module 1-9
Module Perspectives 1-9
Operational Data Definition 1-10
Security Administration 1-10
Assessment Management Definition 1-12

2 Administration Setup

Manage Application Configurations 2-1
Installation Options 2-1

3 Financial Governance Configuration

Configure Module Objects 3-2
Financial Governance Risk Management Configuration 3-2
Manage Perspectives 3-2

4 Module Management

Configure and Manage Modules 4-1
Creating a Module from the Standard Template 4-1
Create a New Module 4-2
Module Object Configuration 4-4
Deleting a Module 4-7

5 Importing Operational Data

Prerequisites 5-2
Preparing the Data Load Spreadsheet 5-2
Adding User-Defined Attributes 5-3
Preparing the New Module Import Template 5-3
Populating the Import Template 5-4
Running the Import Process 5-7
Import Validation 5-8

6 Managing Assessments

7 Security Administration

Security Components 7-1
Privileges 7-2
Duty Roles 7-3
Job Duty Roles 7-3
Primary Data Roles 7-4
Assessment Activity Primary Data Roles 7-4
Composite Data Roles 7-5
Job Roles 7-5
User 7-5
How to Introduce Data Level Security 7-6
Manage Roles 7-9
Constructing Duty Roles 7-10
Constructing Data Roles 7-10
State Action 7-13
Constructing Job Duty Roles 7-15
Constructing Job Roles 7-16

Manage Users 7-17
Define a User with Access to All Operational Data 7-18
Access to Issues within Issue Management 7-19
Security for a New EGRCM Module 7-20
Define Data Roles for the New Module 7-22
Define Perspective Data Roles for Data-Level Security 7-23
Define New Job Roles 7-23
Impact of Changing a Perspective Used in Data Roles 7-25

8 Preparing for a Production Environment

Phase 1: Development (Initial Sandbox/CRP) 8-1
Phase 2: Staging/Preproduction Setup 8-2
Phase 3: Production/Live Maintenance 8-3
Periodic Gold Backup Update 8-3
Installing EGRCM Patch Sets 8-4

A Appendix 1

Troubleshooting Import Data A-1
Understanding Import Error Messages A-1
How to Find Duplicate Names A-2
SQL Error While the Import Runs A-3
Troubleshooting Access A-4
List of Delivered Privileges A-4
Disable the Financial Governance Module A-11

Preface

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

This *Implementation Guide* is meant to provide helpful guidance on the usage of the product. This of this document as a combination FAQ and helpful "Tips and Tricks."

It is a supplement to the official product documentation (such as the *User Guide* and *Installation Guide*), and is not intended to replace it. If discrepancies exist between this *Implementation Guide* and the official product documentation, the guidance and functional commentary provided by official documents supersede any that may be written here.

Disclaimer

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

Other Information Sources

My Oracle Support

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

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

Oracle Enterprise Repository

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

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

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

Documentation Accessibility

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

Comments and Suggestions

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

1

Enterprise Governance, Risk and Compliance Setup Overview

Oracle Enterprise Governance, Risk and Compliance Manager (EGRCM) forms a documentary record of a company's efforts to address the risks it faces and to comply with regulatory requirements.

EGRCM consists of loosely coupled modules; it includes a Financial Governance module by default, and users may employ a standard template to create other modules that address other areas of the company's business.

Within each module, users may define risks to the company's business, controls to mitigate the risks, and other objects, such as the business processes to which risks and controls apply. Moreover, users may create perspectives — hierarchical representations of contexts in which processes, risks, controls, and other objects exist. They may also create user-defined attributes — information added to a given object to extend its definition.

EGRCM enables users to perform periodic assessments of objects and perspectives. As part of assessments, users may conduct company-wide surveys, raise issues when defects are uncovered, and resolve those issues, thus continually reviewing and improving the company's GRC efforts.

Data Types

EGRCM employs varying data types, described by the following terminology:

- Seeded data is metadata delivered with EGRCM, spanning the application. It includes the following data types:
  - Label and header names
  - Seeded lookup table values, such as control assertions or assessment responses (for example, *failed* or *pass*).
  - Perspective hierarchies, such as Organization or Major Process.
  - Security roles: data, duty, and job.
  - Content types.

  - Survey questions.
  - Survey templates.
- Configuration data includes several data types that can be modified by the user, including user-defined attributes, business-object configuration, module perspectives, lookup tables, content types, and URL repository.
- Transactional data refers to data types that describe events or actions that occur within EGRCM. These include the following:
  - The initiation of an assessment and the corresponding results.
  - The initiation of a survey and the responses.
  - The creation of issue and remediation plans.
  - Within the Risk Management work area, the creation and completion of an analysis, evaluation, and treatment.
  - Action items defined within the Process Management work area.
- Operational data encompasses multiple data sources, including legacy data, libraries provided by external sources, and object-specific records defined within the application. Operational data types include:
  - The definition of a process, risk, and control within the seeded Financial Governance module. These definitions can also be referenced as a record.
  - Within custom modules, the definition of objects defined by the user (for example, IT Risks, IT Controls, Assets). This includes definitions of an event and consequences managed within the Risk Management area.

Diagnostic Steps

EGRCM is designed to be incredibly scalable by means of hardware configuration. This means EGRCM performance can often be improved via a hardware change rather than a software change.

Touch points of EGRCM span hardware, software, and network variables. Refer to the Hardware Requirement tab of the *Oracle Governance, Risk and Compliance Applications Support Matrix* for the recommended and supported hardware configuration.

It is highly recommended during implementation planning that sufficient time be allocated for setting up, testing, and troubleshooting environment-specific issues that occur commonly with the many combinations of environments available.

This following is a high-level recommendation for diagnostic steps during environment setup and implementation:

1. Work with Oracle Consulting or an Oracle partner service provider to evaluate your environment and options for an EGRCM installation.

   Consider creating Development, Test, and Production instances. It is highly recommended that the environments for these instances be similar to one another, as varying environments could cause unexpected issues.

   Search for any patches that may need to be applied. EGRCM patches are available on eDelivery and must be applied in sequential order.

2. Refer to the *Support Matrix* for recommended and supported hardware configurations.
3. Look on My Oracle Support for known environment variable issues.
4. Follow instructions in the *Governance, Risk and Compliance Installation Guide* to install EGRCM.
5. Verify that areas of the application are working. (See the *Oracle Enterprise Governance, Risk and Compliance Manager User Guide* for more information.)
    a. Create a new user by making a copy of the seeded *admin* user. Out-of-the-box Review and Approve is not in the workflow. Update this new user to include the Control Reviewer job role.

       For information on adding a job role to a user, refer to step 1 in the Setup Checklist (page 1-4 of this document), and to the "Managing Users" section of the "Managing Security" chapter in the *Oracle Enterprise Governance, Risk and Compliance Manager User Guide*.
    b. Log in as the new user. You need to change the password the first time you log on.
    c. Create a new control within the application.

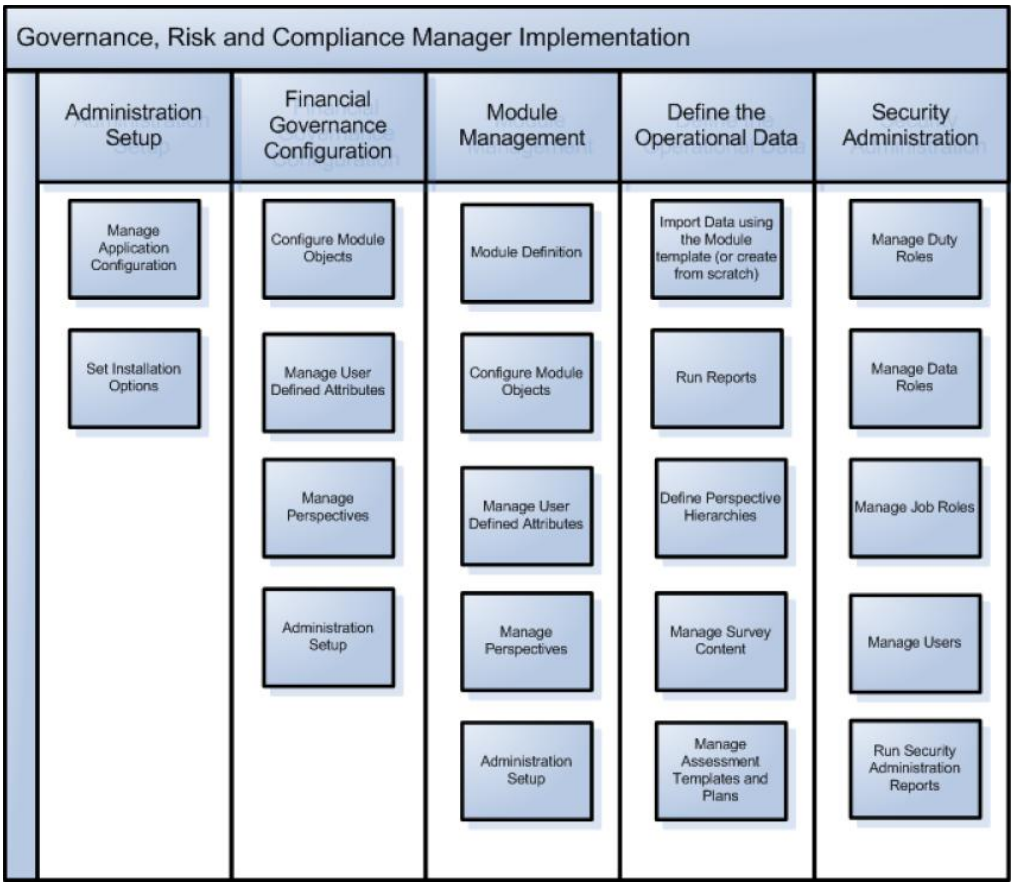
       Does the control appear in the worklist? Validate that the control is in the correct state. If a worklist is not generated, review the user roles to be sure the Control Reviewer job role was added correctly.

       Approve the control through the Review and Approve workflow, and validate it is in the correct state.
    d. Edit the control and select Save. Did the state change to In Edit? Select Submit and then complete the Review and Approval again using the Review and Approval workflow.
6. Create an ad hoc assessment for the control, and select the Audit Test assessment type.

   Does the correct task appear in the worklist? If the worklist is not generated, review the assessment you created and check that the assessment type is set to Audit Test. Validate that the Control Audit Test Assessor Job Role is assigned to this user.
7. Complete the control assessment — out-of-the-box Review and Approve is included for this workflow. Fail the assessment and create an issue against the control assessment. Does the issue appear in the correct state and appear within Issue Management?
8. Use the Run Now feature on the Notifications tab of the Manage Application Configuration page to validate that email is being generated. Be aware that you must have one Worklist entry pending for EGRCM to generate an email. Prior to completing this step, ensure the user has a valid email address.
9. Run the Control Details Report, Control Assessment Report, and Risk Control Matrix Report.
10. If you do not wish for this new user to have Control Reviewer access beyond this verification step, remove the job role.

EGRCM Setup Flowchart

Although you can set up EGRCM in many ways, we recommend that you follow the order suggested in the following flowchart. Some steps are required, and others are optional; perform the optional steps only if you are ready to use the features or business functions implemented by those steps.



Setup Checklist

To set up EGRCM, complete the steps in the following checklist. You must complete the steps identified as required. Complete each of the optional steps only if you want to use the functionality implemented by that step.

Each step is described in further detail later in this document. In addition, the description for each checklist step includes a reference to a section and chapter of the *EGRCM User Guide*, *GRC Installation Guide*, or the current document, where you can find full information about the procedures for completing each step.

Administration Setup

☐ 1 **Required:** EGRCM comes with one configured user, for which both the user name and password are *admin*. Use this user to complete the outlined implementation steps.

The seeded admin user is granted access to all job roles other than review and approval roles, so that the review and approval steps will be skipped during the implementation.

As you validated your installation, you were instructed to create a user based on the admin user (see step 5 of "Diagnostic Steps" on page 1-3). As you complete the implementation, it is recommended that this "admin clone" user also not be assigned reviewer and approver job roles. Assign these job roles only to users who must perform these tasks.

It is recommended that you keep the admin and admin clone users active and do not remove any of their seeded duty and job roles.

Note: Passwords expire, by default every 90 days after being established or reset. A user whose password expires is locked out of the application until the password is updated by a user with access to the security pages, such as the admin user. Ensure that the admin and admin clone users' passwords do not expire on the same day, so that if one is locked out, the other can reset the password.

☐ **2** **Required:** Connect your instance of EGRCM to its database. Typically, connectivity values are set during installation. You would update the values only if your configuration needs to change.

See "GRC Configuration" in the *Oracle Governance, Risk and Compliance Installation Guide*.

☐ **3** **Optional:** EGRCM can connect, and supply information, to Oracle Governance, Risk and Compliance Intelligence (GRCI). For this option to be used, a distinct schema, known as the "Data Analytics" schema, must exist. If you choose to implement this option, use the Analytics tab of the Manage Application Configurations page to provide information EGRCM uses to connect to the Data Analytics schema.

☐ **4** **Optional:** You can choose to integrate the application user administration with your LDAP user repository. This integration allows you to import users defined within the LDAP repository into EGRCM. Integration is a one-way pull from the LDAP repository into EGRCM. Changes made to a user within EGRCM are not pushed back into the LDAP repository. See the *Oracle Governance, Risk and Compliance Applications Support Matrix* for information about supported LDAP repositories. On the User Integration tab of the EGRCM Manage Application Configurations page, provide values required for EGRCM to connect to the LDAP repository.

See "Managing Application Configurations" in the *Oracle Enterprise Governance, Risk and Compliance Manager User Guide*.

☐ **5** **Required:** Several EGRCM-specific options affect the entire installation: the default currency, and the default likelihood and impact models for use in defining proposed risk. These should be set before any data is loaded into the application. These values can be changed after data has been imported. However, this will not change existing data; it will only change the default itself.

See "Managing Installation Options" in the *EGRCM User Guide*.

Financial Governance Module Configuration

☐ **6** Optional: The seeded Financial Governance module objects have several options for configuration. Prior to implementation, think how the module will be leveraged: What assessment activities are required to fulfill the objectives, will events and consequences be defined, are action items used? Out of the box, the configuration options are available (turned on), and this step is required only if some of these features need to be turned off.

See "Module Object Configuration" (page 1-8) as well as "Configuring Module Objects" in the *EGRCM User Guide*.

☐ **7** Required: Financial Governance module administration setup includes:

- Attachment configuration: Attachments are enabled throughout the application. Consider the content types that are used during documentation, testing, and issue remediation. Use Manage Content Types within the Setup and Administration tasks to review the delivered content types and update the list as necessary.
- Configuration of the URL repository: A user-defined attribute (UDA) can be of the link type; it provides the ability to introduce a link to a web site. The URL repository is a set of URLs that can be included in a link UDA. Update the repository with URLs you want to introduce within the EGRCM pages. These links appear in the Additional Details section of a page along with other UDA fields.
- Updating of lookup tables: Some of the lookup tables for attributes on EGRCM objects can be updated with new values. For example, you may wish to add a value for Frequency on Controls, or to add a value for Issue Severity. Not all delivered lookup-table attributes can be modified — see "Managing Lookup Tables" in the *EGRCM User Guide*.
  - If you create a UDA to enable users to select from a set of values, you must create a lookup table that defines the values. Be sure to select the Used for User Defined Attribute checkbox as you define values for the lookup table. Only a table with this indicator turned on can be selected as a Lookup Table for a UDA.
  - Object Type: The Type attribute enables an additional level of categorization for an object. Out of the box, there are no seeded values. When defining these values, consider subgroupings of controls, risks, processes, and so forth. For example, within controls being managed, there are Financial Compliance and IT Security. Two values can be created and used in reporting.

☐ **8** **Optional:** The Financial Governance module includes seeded metadata. Depending on business requirements, additional metadata may be required. UDAs enable users to define custom attributes. Prior to implementation, think how object definitions may need to be expanded. For example, Control Owner and Account values are required. You can define

these additional attributes and associate them to a specific Financial Governance Module object.

For more information on UDAs, see step 20 in this checklist, " Creating User Defined Attributes" on page 4-5, and "Managing User-Defined Attributes" in the *EGRCM User Guide*.

☐ 9 **Required:** Prior to defining perspective hierarchies, think how data-level security applies to the user community. Perspectives are used to define the set of data to which a user has access. Perspective hierarchies provide structure to the objects being managed in the application, by grouping objects together with a common category, which can then be used for sorting, filtering, and reporting. Perspectives are also the drivers for data-level security. EGRCM supports granular data-level security through the perspective in the data role. Data security can be defined at the perspective hierarchy parent or to a specific perspective value. While not every perspective is used for security purposes, this aspect of their usage should always be considered. Therefore, when defining your perspectives keep in mind how you want to manage data security (how you want to segregate your data within the user community) and reporting.

See the "Security Administration" chapter (beginning on page 7-1).

☐ 10 **Optional:** You can load operational data into the application for Financial Governance module objects. Use the Financial Governance Import Template xml file to do this. The data load supported for this release is the initial load of data, which covers objects like processes, risks, controls, perspectives, and so on, and their relationships. Refer to steps 23 and 24 in this checklist.

☐ 11 **Required:** Configure Financial Governance user profiles. Refer to steps 26–30 of this checklist.

Module Management

The following steps are required only when a new module is being defined.

☐ 12 **Required:** EGRCM is delivered with a single template, called the Standard template, which is the foundation for defining a new module. The user must select this template to create a new module. The template provides a defined list of objects and relationships, which can be selected and configured to define a new module. EGRCM provides the ability to modify the seeded objects and their configuration based on the defined parameters within the template.

See "Managing Modules" in the *EGRCM User Guide*.

☐ 13 **Required:** Select objects for the module. Prior to configuring a new module, you consider your current business objective as well as future use to determine which objects to use. For example, if you configure a custom Financial Governance module, and strategy calls for it to include an Objective object in future, you should include that object as part of the new module. This approach enables the user to apply the

additional object easily at the appropriate time. Review the module definition carefully — once a module has been submitted, its definition cannot be modified (although the module can be marked as inactive).

Note: Access to the objects within the module is controlled through grants to users of appropriate job roles in their security profiles. Until a user's security profile has been updated, that user does not have access to the objects. If the module contains an object to be used in future, delay adding the appropriate job role until it is appropriate for users to interact with that object.

☐ **14** **Required:** Configure relationships between the objects that were selected in previous steps. Some key aspects to consider while configuring object associations include these:

- How are the objects related?
- Is the relationship direct, or is there an indirect relationship through another object?

  For example, if you configure Process > Financial Risk > Financial Control, the Process-to-Risk relationship is direct, whereas the Process-to-Control relationship is indirect (it goes through Risk).

  For the Process object, the checkbox for Financial Risk should be turned on, while the checkbox for Financial Control should be turned off. The checkbox for Financial Control should be turned on within the Financial Risk region.

  It's recommended that you first configure the base objects, risk object, and then control objects.

☐ **15** Required: Set labels for the objects. The object labels should be changed as part of the module creation process. It is recommended that the label names be simple and distinct. These names are incorporated into the main navigation and UI pages for this module.

Module Object Configuration

☐ **16** **Required:** The objects (base objects, risks, controls) that define the module's data model have specific configuration options, and each object has specific characteristics to support its business objective. For example, the risk object is designed to support the elements of risk management, while the control object is designed to support test plans and instructions. EGRCM enables the configuration of these objects. Common configuration options include:

- Assessment activity definition: Identifies which assessment activities apply to a specific object.
- Guidance text: Guidance text for assessment activities by seeded object.
- Activity question: Assessment result question.

To refine this configuration, use object-specific configuration options described in steps 17–19.

☐ 17 **Optional:** By default, all the elements for the Risk object are turned on. Prior to implementation, consider how risk management will be used today and in the future. Today users may not need to define events and consequences, but in six months this feature may be required. Events and consequences should remain on; leverage job roles to restrict access to these features of risk management.

See "Managing Objects for the Module" (page 4-4).

☐ 18 **Optional:** Base objects are leveraged to manage a variety of GRC objectives, such as Process, Projects, and Initiatives. Consider how the base object will be used. Open base object configuration options:

- Hide/Show Issue and Remediation (not available for the Financial Governance module object configuration)
- Common Assessment configuration options

If the Issue option is set to Hide, the Issue tab is hidden within the manage object work area. The user cannot create issues for this specific object within the object work area. If the Issue option is set to Hide, the Remediation option is also hidden. If any issue data is associated with the object, the Issue option cannot be changed from Show to Hide.

If the user wants to use the assessment feature for a given object, the Issue options should not be set to Hide for that object, since it is standard practice to create issues when an assessment has failed.

See "Managing Objects for the Module" (page 4-4).

☐ 19 **Optional:** Like those for base objects, configuration options for control objects include Hide/Show Issue and Remediation (once again unavailable for the Financial Governance module) and Common Assessment configuration options. The conditions already described for base-object configuration (see step 18) also apply to control-object configuration.

See "Managing Application Configurations" in the *EGRCM User Guide*.

User-Defined Attributes for Objects within a Module

☐ 20 **Optional:** Define user-defined attributes (UDAs). This feature supports the ability to extend the design for the objects.

Define a UDA for an object within a module to support the addition of other descriptive information needed for the object. For example, suppose that as a business requirement, Risk Owner must be captured as part of a risk object's definition. A UDA would be created to capture this value.

Module Perspectives

☐ 21 **Required:** Review how perspectives are to be managed. If you use new perspective types, you must define these prior to defining the perspective.

☐ **22** **Required:** Perspective hierarchies provide structure to the objects being managed in the application, by grouping objects together with a common category, which can then be used for sorting, filtering, and reporting. Perspectives are also the drivers for data-level security. EGRCM security supports granular data-level security through the perspective in the data role. Data security can be defined at the perspective hierarchy parent or to a specific perspective value. While not every perspective is used for security purposes, this aspect of their usage should always be considered. Therefore, when defining your perspectives keep in mind how you want to manage data security (how you want to segregate your data within the user community) and reporting.

See the "Security Administration" chapter (beginning on page 7-1).

Operational Data Definition

The following steps are required only if legacy data is to be loaded.

☐ **23** **Required:** Operational data can be loaded into the application for Financial Governance and new module objects, through use of an import template Excel spreadsheet. The data load supported for this release is the initial load of data, which covers objects like processes, risks, controls, perspectives, and so forth, and their relationships.

Complete the import template. EGRCM supports two import templates, which are included in the EGRCM 8.6.4 eDelivery package.

- Use the Financial Governance Import Template (FinancialGovernanceImportTemplate.xml) to load data into the Financial Governance module.
- Use the New Module Import Template (NewModuleTemplate.xml) to load data into a custom EGRCM module.

☐ **24** **Optional:** Once the data has been successfully loaded, validate the data by running a few embedded reports. In addition, run the Risk and Control Matrix report to verify the relationships are as intended.

Note: It's recommended that you create a "super user" with access to all operational data associated to perspectives within each module. Log in as this user after the import to review and report on the imported data.

See "Define a User with Access to All Operational Data," page 7-18.

Security Administration

☐ **25** **Required:** The application is delivered with a set of duty roles that are collections of functional tasks or work to be performed within the various areas of the application. The functionality included in each duty role represents the work the user can perform within the job role. What is delivered may or may not align with how your organization segregates work responsibilities, or a delivered duty role may have

functionality you do not wish to use. Review the delivered duty roles. If you need to make changes, create a new duty role by copying one that was delivered, and then removing or adding functionality.

See the "Security Administration" chapter (page 7-1), as well as "Managing Duty Roles" in the *EGRCM User Guide*.

☐ **26** **Required:** Data roles control the data to which users have access within their job roles. At a minimum, each job role needs a data role or a set of data roles to identify the appropriate module, the appropriate object state, appropriate actions, and set of perspectives that align with the data they interact with and the actions they perform against this data. No perspective filters are delivered with the data roles, since they are totally dependent on the perspectives you choose to use for each module. The product is delivered with a set of composite data roles for the Financial Governance module for each of the delivered job roles. Create new custom data roles that reference the seeded composite data roles, and introduce the necessary perspective filters to define the appropriate security access.

Perspective hierarchies must be defined prior to the creation of data roles, since they form the criteria used in the data roles.

See the "Security Administration" chapter (page 7-1).

☐ **27** Job duty roles define the functional privileges for a job. A job duty role is a collection of duty roles that define the tasks performed by a user assigned a job. The product is delivered with a set of job duty roles for each delivered job role that align with the best practices of the functionality performed with each job. However, as with the duty roles, these job roles may not match your organization's requirements. Review the delivered job duty roles. If you need to make changes, create a new job duty role by copying one that was delivered, and then removing or adding functionality. Or, create a new job duty role from scratch.

See the "Security Administration" chapter (page 7-1) as well as "Managing Job Roles" in the *EGRCM User Guide*.

☐ **28** **Required:** Job roles are the security component that combines the functional privileges of the duty role with data roles to form the definition of what tasks are performed against which set of data. The job role is assigned to users. The product is delivered with a set of job roles, but as with the duty roles and job duty roles, these job roles may not meet the requirements of your organization. Review the delivered job roles. If you need to make changes, create a new job role by copying one that was delivered, and then removing or adding functionality. Or, create a new job role from scratch.

See "Job Roles" (page 7-5) and "Constructing Job Roles" (page 7-16), as well as "Managing Job Roles" in the *EGRCM User Guide*.

☐ **29** **Required:** Define users and grant them roles. You can import users from LDAP (see step 4 in this checklist) or define them directly in the application. All functionality must be granted to the user explicitly through the addition of job roles to a user profile.

The product is seeded with one user, called admin, which has been granted all functional job roles except the review and approve job roles. It's recommended that you create a new user by copying the admin user; this should have been done during installation validation (see step 5 of "Diagnostic Steps" on page 1-3). It's recommended that you update this user to have access to all the operational data for all modules — i.e., a super user as discussed in step 24.

See "Define a User with Access to All Operational Data," page 7-18.

☐ **30** **Optional:** Run the security administrative reports to review users and roles:

- Review the Role Assignment report to ensure users are assigned the correct roles.
- Review the Unassigned Perspective Values report to verify that all the appropriate perspectives are referenced within a data role.
- Review the Record Assignment report to see what records a particular user might have access to.
- Review the Inaccessible Records report to see what records may be orphaned based on the security setup.

Assessment Management Definition

☐ **31** **Optional:** Create survey questions and templates as needed to be included in the assessment activity or to be distributed as a general survey to solicit and collect information pertaining to your organization's compliance initiatives.

See "Managing Surveys Explained" in the *EGRCM User Guide*.

☐ **32** **Required:** The objective in using assessment templates and plans is to streamline this process by creating reusable assessment plans. It would be common for users who manage assessment preparation to update or create new assessment plans annually.

See the "Managing Assessments" chapter (page 6-1) of this document as well as the "Managing Assessments" chapter in the *EGRCM User Guide*.

2

Administration Setup

Below is more discussion for each of the planning and installation steps outlined in the "Administration Setup" section of the setup checklist (page 1-4). There are references to other sections of this document or other EGRCM documentation for more detailed instructions.

Use the *Oracle Enterprise Governance, Risk and Compliance Manager User Guide* for help in completing setups.

Manage Application Configurations

Before you begin setting up your application configurations, consider your environment. Will you require various languages? What kind of password security does your company require? Will you import users from LDAP?

Do you want to send daily email notifications to the user community regarding the work they have been assigned? Do you want notifications to include all current assignments or just the new assignments generated since the previous email?

By carefully evaluating your business needs, you can configure your application accordingly for best performance and reporting.

See "Managing Application Configurations" in the *EGRCM User Guide*.

Installation Options

There are a few additional EGRCM-specific options you need to set for your environment. Consider what you want the currency to default to as you build out the application data. If you are using proposed risk, what likelihood and impact models do you want to set as defaults? You will need to wait to set this last option until after you have built out your risk models.

These options are generally set during implementation, but they can be changed at any time. Remember that changing any of these values impacts the entire installation. However, changing the default currency or the risk models will not change the values that already exist within the application data. Any changes made to these

fields take effect only for data entered into the system after the change is made. Existing data is not automatically updated with the new value.

See “Managing Installation Options” in the *EGRCM User Guide*.

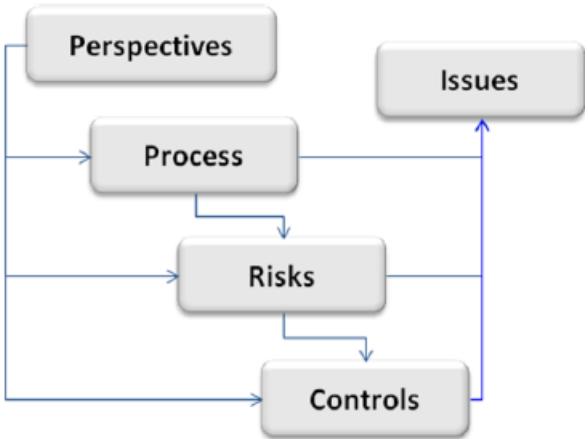
3

Financial Governance Configuration

EGRCM Financial Governance is a seeded module; users will need to stay within the defined parameters of the module. EGRCM supports multiple configuration options for each main object (process, risk, and control) and the module itself. For example, users can hide or display specific features, such as events that are available within the risk object. The user can specify the assessment activities available for the module.

Objects within the Financial Governance module are standard objects defined to support Financial Governance business initiatives. They include Process, Risk, Control, and Issues. (Issues can be created throughout the application.)

The Financial Governance seeded data model can be represented as follows:



The core foundation/definition of these objects is used throughout the application. The difference is how these objects are configured and their relations with other EGRCM objects.

Prior to making any configuration, consider how the module will be used in your organization and how those requirements will change over time. For example, today your organization may not manage risks; however, the business objective is to manage risks within EGRCM within twelve months. In this case, we recommend hiding Risk Management from the users' view by not giving users a job role with access to Risk Management. The object would still be with the module, but no one would have access to view it. Through the restriction of access, unnecessary elements can be removed until the organization is ready for them.

Once the module has been deployed, users can modify or add UDAs, perspectives, lookup table values, assessment activities, and job roles.

For additional information, see “Module Management” (page 4-1).

Configure Module Objects

You will want to configure Financial Governance objects to suit your business initiatives. For information on defining user-defined attributes, see “Creating User-Defined Attributes” on page 4-5. For information on setting administrative options, see “Administration Setup” on page 4-6. Also, consider the following configuration options.

Financial Governance Risk Management Configuration

Consider hiding events, consequences, and treatment plans. Many organizations do not leverage events and consequences. However, evaluate your Financial Governance objects to determine the right configuration pattern for you.

Within Financial Governance, the typical treatment option is Hide and Default. Risk treatment engages the user to define options for risks that fall outside a tolerance level defined by your organization. When treatment is set to Hide and Default, the application leverages a feature by which risks are associated with mitigating controls, and a Related Controls tab is exposed within EGRCM Manage Risk UI pages.

Manage Perspectives

The Financial Governance module does not include seeded perspective hierarchies. You can, however, configure perspective hierarchies, or use the Financial Governance import template to load seeded hierarchies available with the application. Seeded hierarchies include Organization, Major Process, Laws and Regulations, COSO Internal Control Framework, and Financial Compliance Accounts.

You can then associate perspective values with objects in the Financial Governance module. Because perspectives are a main component of data-level security, consider how to utilize them in the most efficient way. As a recommendation, start with one to three perspective hierarchies for data-level security, due mainly to overhead and maintenance concerns.

4

Module Management

EGRCM module management is a comprehensive tool enabling users to configure objects to support multiple GRC business initiatives. For example, a user can configure a custom module to meet specific business requirements for IT governance, ERM, ORM, or audit management.

Module management provides configurability to the user by leveraging a seeded template, which is reusable. They define data models describing common objects — such as process, risks, or controls — and their relationships to one another. By staying within the parameters of a template, users can select only those objects and their relationships that are needed. Prior to defining a module within the application, users should design the module definition, meaning lay out the objects and their relationships so that they meet business requirements.

Configure and Manage Modules

Users can create custom modules from the seeded Standard template, and configure objects within each module.

Basic tasks include:

- Create a module from the Standard template.
- Configure objects within the module.
- Turn object associations on or off.
- View a module by clicking on its name in the module list.

Creating a Module from the Standard Template

The template can support a variety of GRC business objectives. To use it, stay within defined parameters, and use standard objects, relationships, and specific configurability options for each object. A module is created from the template in a single session, so lay the module out and design it before you actually create it in the application. As you design, consider how the module will be used now and in the future. For example, suppose Risk Management will not be used until controls have been implemented fully. In this case, you should include risk objects as part of

the data model, but use security to restrict them from view. Then, when you are ready to use Risk Management, update the appropriate users to grant them access to the risk objects.

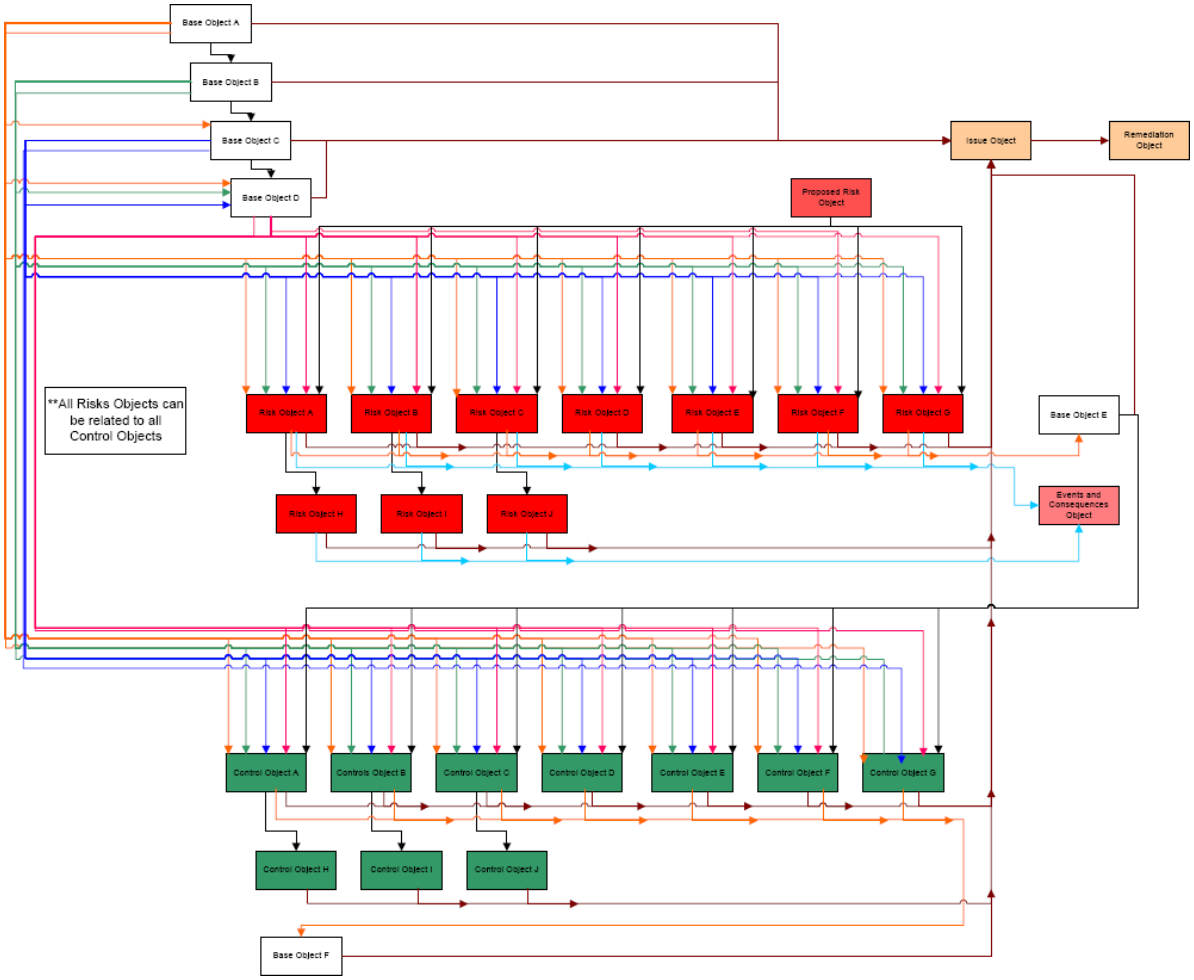
Create a New Module

The creation of a new module includes key steps that must be completed prior to the module being deployed. Each step is a specific element in defining a new module; step 6 also applies to configuring the seeded Financial Governance module.

1. Plan and design the new module prior to configuration.

   Consider the current business objectives as well as future requirements as you design a new module. Determine the objects to be leveraged and their relationships to each other. Define how each object will be configured and the impact this configuration will have on management of records within the application and reporting on those records.

2. Select the seeded Standard template for use as the base for the module. The Standard template provides a list of objects and associated relationships to be chosen and configured as part of the module.



Customers cannot create their own templates. Template selection is limited to seeded templates. Currently, the only seeded template is the Standard template.

3. Select objects. The template provides three object types, and you can configure each in multiple ways:

   - Generic Base Objects. These open objects can be used for defining process, objective, policy, incident, and so forth. Base objects support the following core elements: seeded attributes for object definition, assessment and issue transactions and action items to the specific base object.
   - Risk Type Objects. These support the core elements for managing risks — seeded risk attributes for risk definitions, analysis, evaluation, treatment, assessment and issue transactional data specific to the risk object.
   - Control Type Objects. These support the core elements for managing controls — seeded attributes for control definitions, test plan, test instruction, assessment and issue transactional data specific to the control object.

   The template supports multiple base, risk, and control objects; users can create a specific definition for each object used in the module. For example, a user defines an ERM module requiring three risk and control types. Each object requires a type-specific definition. EGRCM provides a seeded object-specific definition. However, with the business requirements that have been outlined, additional attribute (UDA) configuration is needed to refine each definition. In this example, the user has identified Financial, Human Resource, and Operational risk and control types. Each risk type needs specific risk attributes to properly define the risks being managed; the same requirement applies to the control types. Therefore, the user leverages three open risk objects and the three open control objects with the seeded relationship to the risk objects.

4. Configure the relationships among objects. Use the Standard template, which provides multiple relationship options.

   Consider questions such as these: How are the objects related? Is the relationship direct, or is there an indirect relationship through another object? For example, if you configure Process > Financial Risk > Financial Control, the Process-to-Risk relationship is direct, whereas the Process-to-Control relationship is indirect (it goes through Risk). For the Process object, the checkbox for Financial Risk should be turned on, while the checkbox for Financial Control should be turned off. The checkbox for Financial Control should be turned on within the Financial Risk region.

5. Relabel the objects. This is not required, but it is highly recommended. The template provides generic names for each available object.

   Changing object labels makes them meaningful. For example, you may have selected an object, called RISK_ OBJECT_B in the Standard template, for use in managing IT risk. To make that purpose clear, you can rename the object "IT Risk." Instead of seeing "Risk Object B Management" within the navigator for the module, users will see "IT Risk Management." The relabel text is also used in reports and graphs.

6. Configure the objects. See "Module Object Configuration" (page 4-4).

7. Review the module definition and save it.

Module Object Configuration

Once you've selected objects and created the module, consider how the module will be used and what functionality will be required. Then configure the objects. Complete these procedures:

- Configure objects, including assessment elements if objects require assessment activities.
- Define UDAs.
- Define perspective hierarchies.
- Perform administration setup — manage look-up tables, attachments, and other elements specific to the module.
- Define operational data (as discussed in "Importing Operational Data").
- Define security.

Managing Objects for the Module

Within the module, objects can be configured so that they implement only those features that support your business requirements. The exact options you can configure vary by object.

EGRCM supports multiple assessment activities; Design Review, Operational Assessment, Audit, Documentation Update, and Certification are seeded. In many cases, however, not all these activities need be used. For each object, use an Assessment Activity Definition option to select only those activities that apply. For each activity you select, use a Guidance Text option to configure a description of how to complete the activity, and an Activity Question option to create the question users are required to answer while performing assessments.

Configuration options specific to risk objects include:

- Hide/Show Events and Consequences. Determine whether to hide risk events and consequences; when they are hidden they are unavailable to users and so, in effect, not implemented. An event is a set of circumstances that can place your organization at the defined risk, and a consequence is the outcome or impact of an event. Typically customers use events and consequences to identify causes of the risk, thus supporting the appropriate level of risk analysis.
- Hide/Default options for risk treatment. Treatment functionality engages users to define options for mitigating risks that fall outside a tolerance level defined by your organization. You can select a Hide Treatment option; if so the functionality is unavailable to users and so, in effect, not implemented. Or, if you select a Hide and Default option, the application leverages a feature by which risks are associated with mitigating controls, and a Related Controls tab is exposed within EGRCM Manage Risk UI pages.

For base, risk, and control objects (in a new module only), you may also determine whether to hide issues. If so, the Issue tab is hidden on the manage object page, and users cannot create issues on the object within the object work area. When the Issue option is hidden, Remediation Plan is also hidden. If any issue data is associated with the object, the Issue option cannot be changed from Show to Hide. We do not recommend that you hide issues for objects if the assessment feature is to be used.

Creating User-Defined Attributes

For each object in a given module, you can specify user-defined attributes (UDAs) to extend the object's definition. UDAs are additional metadata associated with records to capture specific business information details. These details can vary across organizations and industries, and the ability to configure them accommodates that variation. UDAs are supported across all objects (risks, controls, etc.) and other items like perspectives and assessments.

Consider how UDAs may capture information beyond the metadata seeded with objects. For example:

- Assessment type: Create a UDA to capture the amount of time spent to complete an audit test.
- Objects: For process, risk, or control, create a UDA to capture the owner for the record being managed.

UDAs support multiple data types, such as String non-translatable, String translatable, Date, and Number. If you want to use a lookup value set with the UDA the UDA should be defined as String non-translatable. Use the String translatable data type when the display type is free-form text or multiple-line text.

See "Managing User-Defined Attributes" in the *EGRCM User Guide*.

Creating Perspective Hierarchies Across Modules

Users can associate perspective hierarchies to objects within a module and specify UDAs for a perspective hierarchy. When a perspective hierarchy is associated with a given object, it appears in records for that object under a special perspectives section. If the perspective hierarchy is marked as required, this information must be provided for records when they are created or edited.

A perspective associates a record with a specific piece of information, and that information can serve as a filtering value as users search through large sets of data or run reports. It can also serve to allow or deny access to a record, based on how data roles are constructed (see the "Security Administration" chapter, beginning on page 7-1).

Specific perspective hierarchies may be associated with specific objects within specific modules. This gives a lot of flexibility in how you set up your perspectives within the modules. Start with a few, simplistic perspectives until you understand better how you may want to use them in future.

You can:

- View perspectives, define their association with the module, and edit the list.
- Associate a perspective with objects within the module, and specify if a perspective is required for each object. This allows the same or different perspectives to be associated to objects within modules. For example:
  - You may want to put perspective values on control objects to identify the region to which each belongs, whereas you may not want this on your corporate risk.
  - You may want to associate the risk object, but not the control object, to a project perspective.

  - You may want the Organization perspective to be used for both the risk and control objects.

- Inactivate perspectives. You cannot delete a perspective if data is associated with it; the delete icon and button are inactive for rows representing these perspectives in the perspective grid. But the perspective can be disabled through use of the status flag, which can be set to Inactive. The version history is updated for this change as well.
- If the perspective is changed from not required to required, nothing happens to the data. This indicates only that the perspective value is required when a save action is initiated on an object.

See the "Perspective Management" chapter of the *EGRCM User Guide*.

Administration Setup

You can use features available under Administration in the Tasks list to modify other elements used with modules:

- Use the Manage Content Types page to designate the types of attachments that can be selected as users attach documents to objects within a module.
- Use the Manage URL Repositories page to designate URLs that may be selected for user-defined attributes of the "link" data type. These UDAs may be associated with module objects.
- Use the Manage Lookup Tables page to extend the list of values for the object attributes. Not all lookup table attributes can be modified. For a complete list, refer to "Managing Lookup Tables" in the *EGRCM User Guide*.

  The object Type attribute is defined in the lookup table. The Type attribute enables an additional level of categorization for an object. Out of the box, there are no seeded values. When defining these values, consider subgroupings of control, risk, process, etc. For example, within the controls being managed, there are Financial Compliance and IT Security.

  The following table contains the names for the Lookup Type for each of the objects that support the type attribute:

Object	Lookup Type
Process	GRCM_PROCESS_TYPE
Risk	GRCM_RISK_TYPE
Control	GRCM_CONTROL_TYPE
Issue	GRCM_ISSUE_TYPE
Remediation Plan	GRCM_REMEDIATION_PLAN_TYPE
Perspective	GRCM_PERSPECTIVE_TYPE

- Use the Manage Lookup Table page to define new lookup tables for UDAs that use the Drop Down control type. The lookup table will contain all the values the user can choose from for the UDA.
- Use the Manage Assessment Results page to tailor the assessment results — the assessment response text.

For additional information, refer to the “Administration Tasks” chapter in the *EGRCM User Guide*.

Deleting a Module

If no records have been created for a module, it can be deleted. This is a typical scenario when the module is created but is not being used. There will not be any instances of objects in the system. Under these circumstances, the user can delete the module. This process deletes the module definition and its association with other objects like perspectives and UDAs. The module is removed from the user list.

It is recommended that, prior to configuring a new module, you create a backup of the environment/database. If the new module definition needs to be removed, you can roll back the environment.

5

Importing Operational Data

EGRCM provides the ability to upload the initial set of operational data by using seeded import templates. Two templates are provided:

- Use the Financial Governance Import Template (FinancialGovernanceImport Template.xml) to load data into the Financial Governance module.
- Use the New Module Import Template (NewModuleTemplate.xml) to load data into a custom EGRCM module.

The import templates support the following objects and associations:

- Processes (base object)
- Risks
- Controls
- Perspectives
- Associations between risk and control — identifying which risks are associated with which controls.
- Associations between process (base object) and risk — identifying which processes are associated with which risks.
- Perspective associations for objects.
- Perspective hierarchies.
- Additional details for objects like user-defined attributes.
- Loading in a library from a provider. To load data, the user must map it to the import template. The data can be incorporated with the initial import.

Only the initial load of data into a module is supported; updating existing application data is not supported. So you are advised to include all relevant data in the import.

The import process does support running multiple initial loads of new operational data, but all the data within a single import run must be new. So if you are loading new controls that have relationships to risks, this is possible only if the risks are also included in the same import run. New Controls cannot be imported with relationships to existing risk or perspective data.

Prerequisites

It is good practice to create a backup of the environment/database just prior to running the import process. This provides the ability to restore the instance and back out the imported data if the data load is not to your satisfaction.

Perspective type codes should be defined. Before the import script is run, the perspective type used for the hierarchy should be defined. The template supports users creating new perspectives with corresponding values within the template worksheet. The associations of these items to the hierarchy is by the perspective type code. The perspective type code does not realign any item within the application, but this code provides the means to tie the perspective hierarchy to values.

- The perspective type code should always be in capital letters with no spaces.
- The application is delivered with several perspective type codes; you can create new codes by using the Manage Lookup Table page. The lookup type is GRCM_PERSPECTIVE_TYPE, and available codes are entered in the Lookup Code column. Add new perspective type codes as new lookup codes for the GRCM_PERSPECTIVE_TYPE. The following table presents the list of seeded perspective type codes:

Lookup Type	Lookup Code	Meaning	Description
GRCM_PERSPECTIVE_TYPE	GRC_PERSP_FLEX	Flex Template Module	Flex Template Module
GRCM_PERSPECTIVE_TYPE	GRC_PERSP_ACTIVITY	Activity	Activity Perspective
GRCM_PERSPECTIVE_TYPE	GRC_PERSP_ORG	Organization	Organization Perspective
GRCM_PERSPECTIVE_TYPE	GRC_PERSP_FIN_ACCT	Financial Governance Accounts	Financial Governance Accounts Perspective
GRCM_PERSPECTIVE_TYPE	GRC_PERSP_LAW_REG	Laws and Regulations	Laws and Regulations Perspective
GRCM_PERSPECTIVE_TYPE	GRC_PERSP_MJR_PROC	Major Process	Major Process Perspective
GRCM_PERSPECTIVE_TYPE	GRC_PERSP_STD_FWK	Standards and Framework	Standards and Framework Perspective

- The perspective type code does not have to be set up in the application lookup table before data is imported, but this is highly recommended.

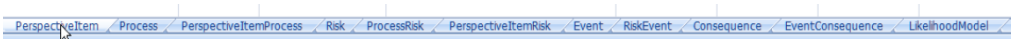
  Until the code has been added into the GRCM_PERSPECTIVE_TYPE lookup table, the UI will not display the perspective. This is a manual step within the application either before or after the data import is completed. Best practice is to do this before the perspective is imported.

For additional information, refer to "Managing Lookup Tables" in the *EGRCM User Guide*.

Ensure that the module has been configured to support the data. For example, set up UDAs and UDA LOVs, and modify lookup tables as necessary. Review the setup and configuration of the module to determine if it is completed. The environment should be set up with all the system data installed and configuration set before the import is initiated. (For example, Hide/Default Treatment for the risk object is configured, UDAs are defined, and so on.)

Preparing the Data Load Spreadsheet

The import template is organized so that each object and each association forms its own tab within the worksheet.



For example, the PerspectiveItem tab includes perspective values, and the Risk tab contains risks that need to be loaded in the database. The PerspectiveItemRisk item identifies the association between risk and perspective.

IDs are used throughout the spreadsheet. These are to relate the data within the spreadsheet. They are not imported and do not impact IDs that exist in the application. Therefore you can use whatever ID system helps you best organize your data. It must, however, be numeric, and you should keep it as simple as possible.

Each object tab (PerspectiveItem, Risk, Control, Process) has a column called STATE_CODE(String)(Required). You can import data in either NEW or APPROVED state.

- If the data is imported in NEW state, the user will have to approve the object data in the application prior to using it.
- If the data is imported in APPROVED state, the user can use the data in the application immediately after import.

It is recommended that you import valid object rows in the APPROVED state.

Adding User-Defined Attributes

User-defined attributes must be created prior to import. The delivered templates contain sample columns for UDAs. Delete unused UDA columns from the spreadsheet for each object prior to import.

Regardless of the number and type of UDA columns in each tab within the seeded import template, you can add more to match the UDAs defined for the objects.

When adding UDA columns to the worksheet, observe the following conventions:

- The UDA columns in the spreadsheet must contain "UDA_" as the prefix.
- This must be followed by the value of the "Name" (not the "Display Name") for the UDA from the definition.
- The name is case sensitive and must match the name used when the UDA was defined.
- The "Double" type in the UDA columns represents numeric values.
- Unused UDA columns must be removed.

For example, suppose the risk definition requires a risk UDA, for which the display name is Cost but the name is Remediation Cost. The UDA column in the import spreadsheet would be "UDA_Remediation Cost," with (String) or (Double) following the name.

Preparing the New Module Import Template

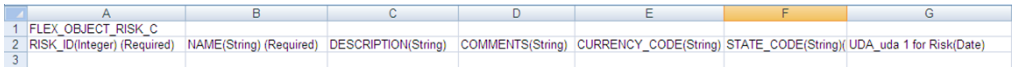
If you are preparing the New Module Import Template, there are a few other considerations:

- The template contains multiple tabs for base objects, risk objects, and control objects. The A and B instances of these objects are provided (for example FLEX_OBJECT_RISK_A and FLEX_OBJECT_RISK_B). If you are completing both the A and B worksheets for an object, the ID you enter within each tab must be unique. It is permitted to have the same ID number for a risk and a control object; however, do not use the same ID number for a row in the FLEX_OBJECT_BASE_A worksheet and in the FLEX_OBJECT_BASE_B worksheet.

- There are many objects within the standard template, but the New Module Import Template is delivered with just the A and B objects for base object, risk, and control. If the new module is to use any other objects, you need to add them to the template.

  For example, add FLEX_OBJECT_RISK_C by doing the following:

  1. Insert a new worksheet following FLEX_OBJECT_RISK_B.
  2. Change the name of the worksheet to FLEX_OBJECT_RISK_C.
  3. Copy all the contents of FLEX_OBJECT_RISK_B into the new worksheet.
  4. Change the name of cell A1 from FLEX_OBJECT_RISK_B to FLEX_OBJECT_RISK_C.
  5. Remove the data rows from this worksheet, leaving only rows 1 and 2.
  6. Complete the UDAs for FLEX_OBJECT_RISK_C as described in "Adding User-Defined Attributes" (page 5-3).



	A	B	C	D	E	F	G
1	FLEX_OBJECT_RISK_C						
2	RISK_ID(Integer) (Required)	NAME(String) (Required)	DESCRIPTION(String)	COMMENTS(String)	CURRENCY_CODE(String)	STATE_CODE(String)(	UDA_uda 1 for Risk(Date)
3							

  Adapt these steps for other FLEX_OBJECT_BASE, FLEX_OBJECT_RISK, or FLEX_OBJECT_CONTROL objects needed for the new module.

- Remove any unused FLEX_OBJECT_BASE_A/B, FLEX_OBJECT_RISK_A/B, or FLEX_OBJECT_CONTROL_A/B that are not needed for the module.
- Enter all perspective-to-flex-base-object relationships in the PerspectiveItemProcess tab. The ID for all the types of process or base object must be unique across the set of base objects. Note: process is a base object.
- Enter all the perspective-to-flex-risk-object relationships on the ProcessRisk tab. The ID for all the types of risk objects must be unique across the set of risk objects.
- Enter all the perspective-to-flex-control-object relationships on the PerspectiveItemControl tab. The ID for all the types of control objects must be unique across the set of control objects.
- Enter all relationships between flex base object, flex risk, and flex control in the ObjectRelation tab.

  Each relationship is defined as a parent-and-child pair. Specify the Parent Object Type, Parent Object ID, Child Object Type and Child Object ID. The object-type values are the names of the objects, such as FLEX_OBJECT_BASE_A, FLEX_OBJECT_RISK_A, FLEX_OBJECT_CONTROL_A. The ID is the ID for the object on the worksheet as used in any other relationship definition. The ID for all types of risk and control objects must be unique across the set of objects.

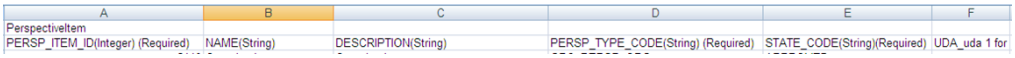
Populating the Import Template

As you populate the import template, keep the following in mind:

- The first row of a worksheet identifies the information you are adding. The second row identifies data columns; in addition to column name, it identifies the

column type (String, Integer, Data, and so forth) and whether the field is required in the database. Do not remove these rows or change any of the data in them (except for the UDA columns, as discussed in "Adding User-Defined Attributes" on page 5-3).

Required fields are marked accordingly. Note, however, that the NAME field is always required, whether it's marked that way or not.



	A	B	C	D	E	F
1	PerspectiveItem					
2	PERSP_ITEM_ID(Integer) (Required)	NAME(String)	DESCRIPTION(String)	PERSP_TYPE_CODE(String) (Required)	STATE_CODE(String)(Required)	UDA_uda 1 for

- The first column of each spreadsheet contains ID values, and each value must be unique within its spreadsheet. For example, populate the column with sequential numbers starting at 1. This column is not saved in the database, but plays an important role in identifying associations between objects on the spreadsheet. Keep in mind that the ID for all types of the same object (base, risk, and control objects) must be unique across the set of objects.
- The seeded import templates contain some sample rows, as an aid to illustrate how to complete the template. Remove this sample data before running the import.
- Populate the Perspective Item tab with perspective values:
  - Complete the PerspectiveItem tab with the values that are associated to the objects (risks, controls, process).
  - Values in the PerspectiveItem tab are loaded without any relationship to a perspective hierarchy. This supports the ability for a perspective value to be included in more than one perspective hierarchy.
  - Set the PERSP_TYPE_CODE to a value that indicates a perspective hierarchy type. Each hierarchy designates a type code (and any number of hierarchies may use a given code), but each hierarchy can contain only values of the same type code.

  The following illustration shows the completed perspective item tab:

	PerspectiveItem				
1	PERSP_ITEM_I	NAME(String)	DESCRIPTION(String)	PERSP_TYPE_CODE(String) (Required)	STATE_CODE(String)(Required)
2	1	Division1	Division 1 Description	GRC_PERSP_ORG	APPROVED
3	2	Division2	Division 2 Descrption	GRC_PERSP_ORG	APPROVED
4	3	Division3	Division 3 Description	GRC_PERSP_ORG	APPROVED
5	4	Region1	Region 1 Description	GRC_PERSP_ORG	APPROVED
6	5	Department1	Department 1 Description	GRC_PERSP_ORG	APPROVED
7	6	Department2	Department 2 Descprition	GRC_PERSP_ORG	APPROVED
8	7	Assessment Cycles	Assessment cycles	ASSESSMENT_CYCLE	APPROVED
9	8	Quarter 1	Quarter 1 Assessment Cycle	ASSESSMENT_CYCLE	APPROVED
10	9	Quarter 2	Quarter 2 Assessment Cycle	ASSESSMENT_CYCLE	APPROVED
11	10	Quarter 3	Quarter 3 Assessment Cycle	ASSESSMENT_CYCLE	APPROVED
12	11	Quarter 4	Quarter 4 Assessment Cycle	ASSESSMENT_CYCLE	APPROVED
13	12	Annual	Annual Assessment Cycle	ASSESSMENT_CYCLE	APPROVED

  The first three rows show that Division 1, Division 2, and Division 3 are perspective values to be added to the seeded Organization perspective. The PERSP_TYPE_CODE is the one delivered for the Organization hierarchy (GRC_PERSP_ORG).

  Rows 7–12 contain values for a new perspective to be used for the assessment cycle. The PERSP_TYPE_CODE for these values is a new type code — ASSESSMENT_CYCLE — that will need to be added to the lookup table for GRCM_PERSPECTIVE_TYPE.
- Populate the PerspectiveTree tab. The tree is the definition of the perspective; it contains information entered in the header section of the Manage Perspective

hierarchy page. The following illustration shows perspective tree and perspective hierarchy.

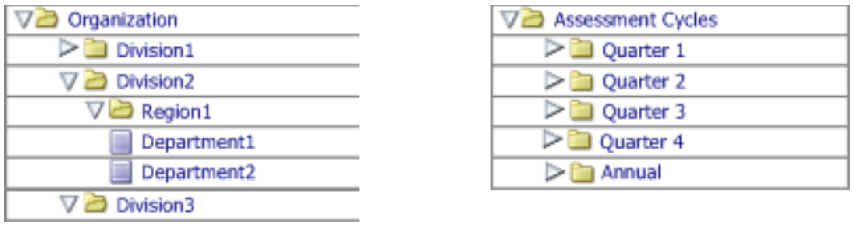
PerspectiveTree					
PERSP_TREE_ID (Integer) (Required)	NAME(String)	DESCRIPTION(String)	PERSP_TYPE_CODE(String) (Required)	STATE_CODE(String)(Required)	
1	Assessment Cycle	Assessment Cycle	ASSESSMENT_CYCLE	APPROVED	

The PERSP_TYPE_CODE for the hierarchy must be the same as the code for the values it contains. In this example, PERSP_TYPE_CODE is ASSESSMENT_CYCLE, which matches the assessment cycle values shown earlier for a new assessment-cycle perspective.

- Populate the PerspectiveHierarchy tab, which expresses the relationships among the values within the perspective. The following illustration shows the completed spreadsheet:

PerspectiveHierarchy			
PERSP_ITEM_NAME(String)(Required)	CHILD_NAME(String)	TREE_NAME(String)(Required)	ROOT(String)(Required)
Organization	Division1	Organization	Y
Organization	Division2	Organization	Y
Organization	Division3	Organization	Y
Division2	Region1	Organization	N
Region1	Department1	Organization	N
Region1	Department2	Organization	N
Assessment Cycles	Quarter 1	Assessment Cycle	Y
Assessment Cycles	Quarter 2	Assessment Cycle	Y
Assessment Cycles	Quarter 3	Assessment Cycle	Y
Assessment Cycles	Quarter 4	Assessment Cycle	Y
Assessment Cycles	Annual	Assessment Cycle	Y

PERSP_ITEM_NAME is the parent perspective value, and CHILD_NAME is the perspective value subordinate to it. Set ROOT to Y when the perspective value listed in the PERSP_ITEM_NAME is the top value in the hierarchy. Set ROOT to N for all other relationships. Once loaded, the Organization and Assessment Cycle perspectives look like this:



- The Financial Governance Import Template contains seeded perspectives. If you do not plan to use these hierarchies, you can remove them from the worksheet, but you must remove the values from the Perspective Item, Perspective Tree, and Perspective Hierarchy tabs that make up the complete perspective definition.
- Populate each object worksheet with operational data appropriate to its object. Each worksheet provides the ability to add user defined attribute values into the database. During preparation, UDA columns were added to the import template (see “Adding User-Defined Attributes” on page 5-3). Complete them with the appropriate values.
- The import process supports the import of multiple values for a single attribute when appropriate, as in the case of control assertions. When needed, enter all the appropriate values separated with commas. Do not include spaces before or after commas. For control assertions, for example, a proper entry would be VALUATION_ALLOCATIONS,RIGHTS_AND_OBLIGATIONS,PRESENTATION_DISCLOSURE,EXISTENCE_OCCURRENCE. (For more on control assertions, see “Creating New Controls: Critical Choices” in the *EGRCM User Guide*.)

- Populate the worksheets for object associations. This involves identifying associations between objects, like risks that have associated controls, or controls belonging to a given organization.

  The following illustration shows associations between controls and perspective items. The IDs on this page match IDs on the Control and Perspective Item tabs. For example, the control ID 1 is associated with two perspective items, Division1 and Region1 (as shown in the perspective-item illustration on page 5-5).

  Controls 1, 2, and 3 share a perspective value, which is represented by their all being associated with perspective ID 4 in the bottom three rows of this example.

PerspectiveItemControl	
PERSP_ITEM_ID(Integer)	CONTROL_ID(Integer) (Required)
1	1
2	2
3	3
4	1
4	2
4	3

- Make sure that the import template is not saved with empty cells highlighted. Otherwise the import will generate Null error messages.
- Make sure there are no duplicates in the Name and ID columns in all the tabs. Otherwise the import will generate duplicate error messages. See "How to Find Duplicate Names" (page A-2).
- Remove all data filters, if any, from each tab sheet.
- Be sure the template is saved as XML Spreadsheet 2003 (*.xml).

Running the Import Process

To run the import process, log into the application. Select Setup and Administration in the Navigator, and then select Data Migration in the Module Management list of tasks. In the Data Migration page, click the Import Data File button.

The import process has the following constraints:

- The process supports the initial load of the module data. It does not support the updating of existing data. However, the import can be run multiple times to load new data.
- The imported data will not go through a review and approval process.
- The import utility supports loading data in either of two states, New or Approved.
  - Imported records will exist immediately with the status/state of "Active/ Approved" if imported with the APPROVED state code.
  - Imported records will exist immediately with the status/state of "Active/ New" if imported with the NEW state code. In this case, they will have to be approved within the application.
- In the imported data log, the Created By value will be set to the username of the user who ran the import.

Import Validation

To ensure data integrity, the import process performs the following data validation:

Validation	Error Message
All the required fields must be listed as columns within worksheet for the object.	Required Attribute is missing within the template (attribute name, sheet name, row number)
The attribute type specified in the column header in the import template must match data type of the attribute.	Wrong attribute type specified for the attribute (attribute name, attribute type, sheet name, row number)
The Perspective or the Object specified in the association is not found within the import template.	Object referenced is not found (entity referenced, attribute name, attribute value, sheet name, row number)
The value for the attribute in the import file must match the data type of the attribute. I.e. if the attribute is numeric, the import value cannot contain characters.	Attribute value given does not match the attribute data type; valid data types are String, Integer, Long, Double, Date and Timestamp (attribute name, attribute type given, sheet name)
The object names within the template for a specific object type must be unique.	Attribute Value given makes the row duplicate (attribute name, attribute value, sheet name, row number, previous row number)
All rows must have unique key values specified within the import file. For example, you cannot have 'Accounts Payable' as the perspective item name in the row for the Organization perspective type and for the Major Process perspective type.	Attribute Values given makes the row duplicate (attribute name, attribute value, attribute name 2, attribute value 2, sheet name, row number, previous row number)
The UDA name listed within the template must already be defined as a UDA definition.	Attribute given is not defined (attribute name, sheet name)
The UDA name must be defined for the object worksheet it is listed on. For example, a UDA defined for control, cannot be used for Risk.	Wrong object type defined for the UDA attribute (attribute name, sheet name)
The data type listed in the column header for the UDA must match the UDA definition.	Data type given for the UDA attribute does not match the data type defined (attribute name, sheet name)
The attribute values must match one of the values within the LOV when supported by a Lookup table.	Attribute value given is not in the valid list of values (attribute name, attribute type, sheet name, row number)
Import template must be saved as 'XML Spreadsheet 2003(*.xml) format within excel.	Import file given is not an XML spreadsheet
Import xml template can only be edited by excel and 'XML spreadsheet 2003(*.xml) is the only valid format type.	XML parser exception occurred; see log.
Any other unexpected system error encountered	Unexpected exception occurred; see log.
All required fields must be completed for a new object	Value is missing for a required attribute (attribute name, sheet name)
The object name cannot already exist within the application.	Object already exists with the name given (attribute name, attribute value, sheet name, row number)

See also "Troubleshooting Import Data" (page A-1).

6

Managing Assessments

Objects such as risks and controls require periodic review of how they are defined and implemented to ensure that the appropriate levels of documentation and controls are in place. Within EGRCM, the Manage Assessment tool helps to support this process of testing, documentation, gathering evidence, and so forth. Typically assessments require planning and proper resource allocation. The objective is to use assessment templates to streamline the process by creating reusable assessment plans. It would be common for users who manage assessment preparation to update or create new assessment plans annually.

When defining an assessment template, consider the assessment activities that need to be performed. (Examples of assessment activities are audit, operational, documentation, etc.) Each object has a set of assessment activities specific to assessing that object type. For example, if there are specific assessment activities for quarterly versus annual assessment, two assessment templates would be defined to reflect the specific activities.

When defining an assessment plan, consider the criteria of the assessment and the coinciding assessment template. The objective is to define reusable assessment plans that can be initiated throughout the year, thus reducing the time required to manage these activities.

EGRCM supports multiple assessment activities (for example audit, design, and operational). However, not all business functions require all of these activities. As a part of EGRCM object configuration, determine which assessment activities are to be used, and activate only those activities. EGRCM does support the ability to make modifications — adding or removing assessment activities after the module is active.

While you define your perspective hierarchies, think about how you can use them to streamline your assessment plans and activities. Grouping EGRCM objects in a hierarchical tree will enable you to manage your assessments from a categorization level, versus an individual or fragmented approach.

7

Security Administration

GRC security employs a standard role-based access control (RBAC) model. You can combine security components — privileges, data roles, duty roles, and job roles — to define "who can do what on which set of data." The "who" is a user assigned a job role. Within the job role, two types of duty role (which ultimately invoke sets of privileges) determine the "what," and data roles determine the "which set of data."

This structure supports reusability: To define new job roles, you can use a given functional-access definition (set of duty roles) over and over again with varying data-access definitions (sets of data roles). Likewise you can use a given data definition with any number of functional definitions. Keep the concept of reusability in mind as you build out duty and data roles.

Security Components

GRC assigns individual users distinct combinations of rights to data and to functionality. To define access to functionality, it uses these components:

- A "privilege" is a specific feature GRC can make available to users.
- A "duty role" is a set of privileges. Each duty role defines one or more tasks a user can complete in the application — for example creating controls, or approving changes to them.
- A "job duty role" is a set of duty roles. It encompasses the functionality a user needs to do a large-scale job such as Control Manager or Risk Manager.

To define access to data, GRC uses these components:

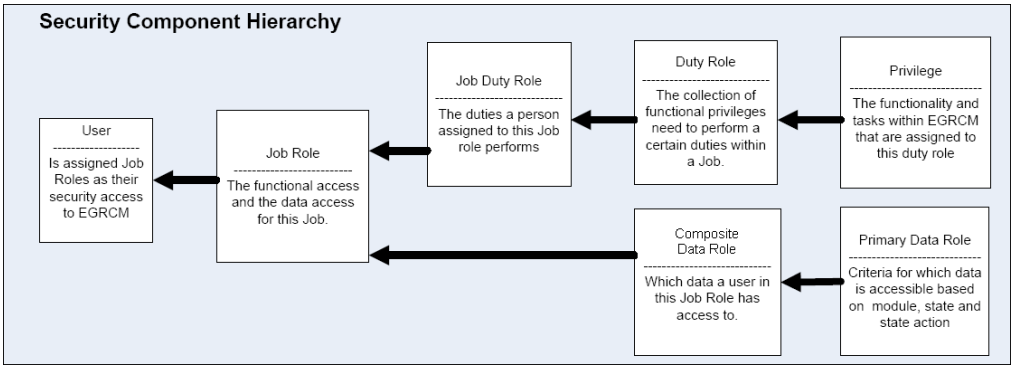
- A "primary data role" defines a set of data that satisfies (in most cases) three conditions: The data belongs to a specified module; exists at one or more specified states, such as New, In Edit, or Awaiting Approval; and is subject to a particular action, for example Create or Delete. A primary data role that supports assessment activities additionally grants access only to data associated with a specified value for a seeded perspective called Activity Type.
- A "composite data role" is a set of primary data roles. It defines the data to which a user can apply the functionality granted in a job duty role. Users may create "custom perspective data roles," each of which combines a composite

data role with a filter that allows access only to data associated with a specified perspective value.

To combine functionality and data access, GRC uses these components:

- A "job role" comprises a job duty role and a composite data role (or custom perspective data role).
- Each EGRCM user is assigned one or more job roles.

The following figure illustrates the relationships among these components.



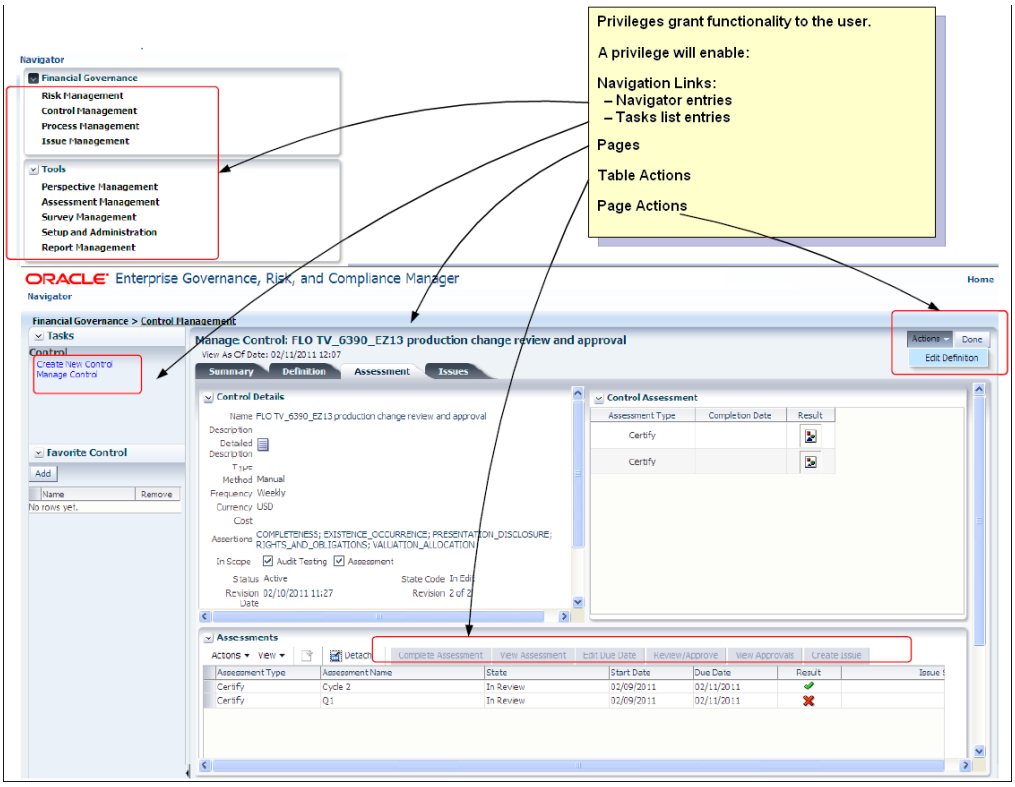
Privileges

A privilege is the most granular aspect of the functional access within the application. The privilege is a reference to a specific application resource and is the means to grant functional access to the user. Each privilege has a name that describes the functionality it grants, a navigator entry that identifies the navigator component within which it is included, and an activity that identifies the type of activity within the application it is part of. The following table contains a few privileges for controls:

Navigator	Activity	Privilege
Control Management	Control Management	View Control
		View Control Approval History
		View Control Assessment Approval History
	Control Maintenance	Create Control
		Delete Control
		Create Control from Related Components
		Edit Control
		Create Issue for Control Definition
		Review Control Changes
		Approve Control Changes
	Control Assessment	Create Control Adhoc Assessment
		Create Issue for Control Assessment

Privileges are seeded within the application and cannot be created by the user.

A privilege grants the user access to a page, but it also enables navigation links as well as page and table actions. The following diagram illustrates elements of the user interface that can be enabled by a privilege.



Refer to the Appendix for a complete list of privileges.

Duty Roles

A duty role is a collection of privileges. Each represents a set of functional tasks needed for a unit of work within the application — a particular aspect of work to be performed. The following list presents a few Control duty roles, and their privileges:

- Create New Control: Privileges include Create Control and Delete Control.
- Control Management: Privileges include Create Control, Create Control from Related Components, and Edit Control
- Control Viewing: Privileges include View Control, View Control Approval History, and View Control Assessment Approval History.
- Review Control: Includes the Review Control Changes privilege.
- Approval Control: Includes the Approve Control Changes privilege.

Job Duty Roles

The job duty role is a type of job role that defines the functionality for a job, but does not contain the data access roles. It is a collection of duty roles. The job duty role represents the full set of functionality a user needs to be granted to perform a large set of integrated tasks.

For example, the Control Manager Job Duty Role contains the following duty roles: Create New Control, Control Management, Create Issue for Control within Control Management, Create Issue for Control Assessments, Control Viewing, Control Assessment Result Viewing, and Control Reporting.

Primary Data Roles

The primary data role is the most granular level of data access. It contains filters that select operational data according to its base attributes:

- The module with which the data is associated.
- The state of the data within the application workflow.
- The state action that can be performed against the data in its identified sate — for example, Create/Edit, Delete, or View.

There is a primary data role for each basic action for each of the objects.

For example, an Edit Control Primary Data Role contains three filters, and the role grants access to data for which all three filters evaluate to true:

- A filter selects data for which a Module attribute is set to Financial Governance.
- A filter selects data for which a State attribute equals any of the following: New State Control, In Edit State Control, Rejected State Control, or Approved State Control.
- A filter selects data for which an Action attribute equals Edit.

Oracle has provided a complete set of primary data roles for all the core entities. The naming convention for primary data roles is: *"State Action" "Entity Name" Primary Data Role* (for example, Edit Control Primary Data Role). This distinguishes them from other data roles.

Assessment Activity Primary Data Roles

A primary data role that supports assessment activity contains a fourth filter to identify the type of activity the role supports; each grants access only to data appropriate to its type of assessment activity. The filter specifies a value for a system perspective called Activity Type. A primary data role that includes any Assessment Results state must include a filter for the Activity Type perspective.

The Activity Type perspective is not available within Perspective Management and is used only for the definition of assessment activity primary data roles.

For example, Control supports four types of assessment activity: Operational Assessment, Design Review, Audit Test, and Certification. So instead of one primary data role for Complete Control Assessment, there are four, one for each assessment activity type.

All four contain three identical filters:

- A filter selects data for which a Module attribute is set to Financial Governance.
- A filter selects data for which a State attribute equals any of the following: New State Control Assessment Results, In Edit Assessment Results, Rejected State Assessment Results.

- A filter selects data for which an Action attribute equals Edit.

But each of the four contains a distinct Activity Type filter:

- Complete Control Operational Assessment Primary Data Role contains a filter in which the Activity Type perspective equals Operational Assessment.
- Complete Control Design Review Assessment Primary Data Role contains a filter in which the Activity Type perspective equals Design Review.
- Complete Control Audit Test Assessment Primary Data Role contains a filter in which the Activity Type perspective equals Audit Test.
- Complete Control Certification Assessment Primary Data Role contains a filter in which the Activity Type perspective equals Certification.

Composite Data Roles

A composite data role is a collection of primary data roles needed for a particular job. It contains filters, each of which sets a Data Role attribute equal to one of the constituent primary data roles. Thus the composite role collects the data access provided by the primary roles.

For example, Control Manager Data Role contains eight filters that specify the Edit Control Primary Data Role, View Control Primary Data Role, View Control Operational Assessment Results Primary Data Role, View Control Design Review Assessment Results Primary Data Role, View Control Audit Test Assessment Results Primary Data Role, View Control Certification Assessment Results Primary Data Role, Create Control Primary Data Role, and Delete Control Primary Data Role.

When a composite role cites more than one primary role, it uses OR logic. In other words, the composite role grants access to data when that data matches criteria specified for any one of its constituent primary roles.

Each seeded composite data role bears the name of the job duty it supports, but ends with the suffix *Data Role*.

Job Roles

The job role is the combination of functional access and data access. It references one or multiple job duty roles and a composite data role, defining the complete set of functional and data access needed for a job.

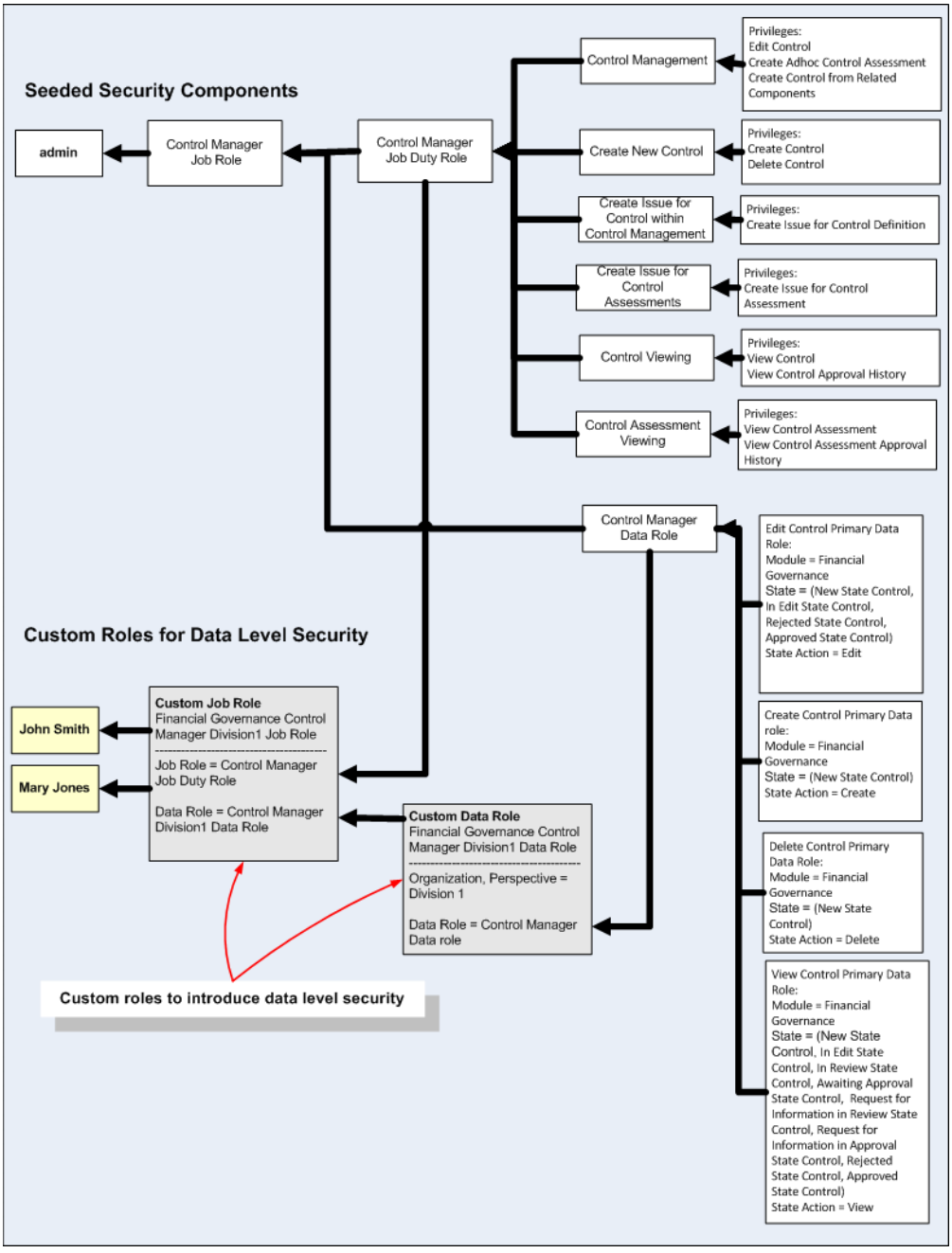
For example, the Control Manager Job Role includes the Control Manager Data Role and The Control Manager Job Duty Role.

User

The user is the actual person using the application. Each user has a security profile that includes identifying information and defines the user's access to the system. A user can have one or multiple job roles. When signing into the application, the user is granted access that is the combination of all the job roles the user is given.

How to Introduce Data Level Security

The following example illustrates how to leverage the seeded security components to define data-level security for the user community.



The unshaded components are seeded, and represent the Control Manager job role, which grants the ability to create, edit, delete, and view controls. You can define data access so that users can perform these actions only on controls associated with a perspective value. To do so, you create a custom perspective data role, and then include that role within a custom job role.

In the example, it's assumed that the Organization perspective includes values that divide a company into divisions, one of these values is Division 1, and your purpose

is to create custom roles that focus a Control Manager on controls associated with Division 1.

First, create a custom perspective data role. As fully configured, the role might look like this:

Name: Financial Governance Control Manager for Division1 Data Role

Description: Access to create and maintain controls in Division1

Filter Name	Object	Attribute	Condition	Value	Include/Exclude
Division1	Perspective	Organization	Equals	Division1	Include
Control Manager	Data Attributes	Data Role	Equals	Control Manager Data Role	Include

The role contains two filters:

- A Control Manager filters sets a Data Role attribute equal to Control Manager Data Role. This provides access to data defined by the seeded Control Manager composite data role.
- A Division1 filter specifies that the Organization perspective be equal to Division1, thus limiting access to data associated with the Division1 value of the Organization perspective.

The system uses AND logic to combine the perspective criterion with the Control Manager Data Role criteria, and so grants access only to data for which both filters evaluate to true. In other words, data must meet all of these conditions:

- The perspective value associated to a control must equal Division1 (the condition of the Division1 filter).
- The control must exist in the Financial Governance module (a condition of the Control Manager filter).
- The control must be in one of the following state/action combinations (a condition of the Control Manager filter, because each combination is defined in one of the primary data roles that belong to the Control Manager Data Role):
  - Control State equals any of New State Control, In Edit State Control, Rejected State Control, or Approved State Control, AND Action equals Edit.
  - Control State equals New State Control AND Action equals Delete.
  - Control State equals any of New State Control, In Edit State Control, In Review State Control, Awaiting Approval State Control, Request for Information in Review State Control, Request for Information in Approval State Control, Rejected State Control, or Approved State Control AND Action equals View.

Second, create a custom job role that references the new custom perspective data role: Copy the seeded Control Manager job role (and give the copy a new name), remove the seeded data role from the copy, and add in the new data role.

Name: Financial Governance Control Manager for Division1 Job Role

Description: Maintain controls for Division1

Role Type	Role
Job Role	Control Manager Job Duty Role
Data Role	Financial Governance Control Manager for Division1 Data Role

Impact of Defining the Perspective Filter in a Separate Data Role

To implement data-level security, you created a data role that combines a perspective filter with an existing composite data role definition; you then included that data role (and a job duty role) in a job role. Do *not* instead include a perspective filter in its own data role, then create a job role that consists of a job duty role, a composite data role, and the perspective-filter data role. This would produce completely different results, because the application uses OR logic to evaluate a job role that contains multiple data roles.

For example, suppose you create a data role containing only one filter, which specifies the Division1 value of the Organization perspective:

Name: Division1 Data Role

Description: Access to Division1

Filter Name	Object	Attribute	Condition	Value	Include/Exclude
Division1	Perspective	Organization	Equals	Division1	Include

Suppose also that you include this role along with seeded job duty and data roles in a job role:

Name: Financial Governance Control Manager for Division1 Job Role

Description: Maintain controls for Division1

Role Type	Role
Job Role	Control Manager Job Duty Role [seeded]
Data Role	Control Manager Data Role [seeded]
Data Role	Division1 Data Role

This configuration would produce results that differ from the data-level-security example illustrated on page 7-6, granting access to all controls for which either of the following is true:

- A control is associated with the Division1 perspective value, even if it does not satisfy conditions defined in the Control Manager Data Role.
- A control satisfies conditions defined in the Control Manager Data Role, even if it is not associated with the Division1 perspective value: It exists in the Financial Governance module AND in one of the following state/action combinations:
  - Control State equals any of New State Control, In Edit State Control, Rejected State Control, or Approved State Control, AND Action equals Edit.
  - Control State equals New State Control AND Action equals Delete.
  - Control State equals any of New State Control, In Edit State Control, In Review State Control, Awaiting Approval State Control, Request for Information in Review State Control, Request for Information in Approval State Control, Rejected State Control, or Approved State Control AND Action equals View.

Because the Division 1 Data Role criterion is not included with the Control Manager Data Role criteria, the user has access to view, but take no other actions on, controls whose perspective value is equal to Division1.

Manage Roles

Before you begin setting up your roles, consider who will use EGRCM and for what purposes. This will be the foundation for job duty roles. Examples include:

- Control Manager. A user in this role is responsible for the administration aspects of the compliance program. As an administrator, the user creates and maintains controls, issues, perspectives, and process.
- Control Assessor. A user in this role works independently of management to perform testing against the controls. A user in this role can also create and review issues, as well as participate in the assessment activities against controls.
- Risk Manager. A user in this role is responsible for the management aspects of risk management. This user is responsible for creating and maintaining definitions of risk, events, and consequences and the various risk models.
- Line of Business Manager. A user in this role is a manager (a line of business head, senior manager, or departmental manager) who leads a group of business process owners. This user makes sure the team provides necessary information to the audit/compliance group on time, and makes sure that related documentation is up to date. The user may be involved in periodic rollup certifications or surveys against the entire area, but does not operate at the process level.
- Process Manager. A user in this role owns one or more processes that are in the scope of the financial compliance program and may impact the accuracy of the financial reports. This user is responsible for maintaining the accuracy of the process documentation, evaluating risks to the processes, and identifying controls necessary to mitigate the risks; performs quarterly attestations for management on the state of the processes he owns; and participates in the annual assessment of the design and operational effectiveness of processes.
- Internal Auditor. A user in this role is responsible for executing the internal audit plan for financial compliance; works independently of management to determine the operational status of controls, completeness and accuracy of documentation; and delivers work papers and evidence that is often leveraged by the external auditor.
- Issue Manager. A user in this role is responsible for managing issues, and in that capacity creates and maintains issues and remediation plans.
- Perspective Manager. A user in this role has access to Perspective Management and is responsible to manage perspectives across EGRCM objects and modules. The user maintains hierarchies and perspectives within the hierarchies.
- Assessment Manager. A user in this role has access to Assessment Management to create and manage assessment plans and all assessments. This user also has the authority to initiate and close active assessments.
- Survey Manager. A user in this role has access to Survey Management to create and manage survey templates and surveys. This user also has the authority to initiate and close surveys.
- System Administrator. A user in this role has the responsibility to define and maintain the setup and configuration data for the EGRCM instance.
- External Auditor. A user in this role is someone outside the organization who performs audit testing and views control information.

Start your security model off small, and then as you see how the users will interact with tasks pertaining to your business objectives, you can continue to refine security access. It is easier to add granularity in the security model than it is to remove excess granularity.

Constructing Duty Roles

The duty role defines what a user can do within the application. A set of duty roles is provided. Each role is defined as logical groupings of a task a user performs within the various areas of the application — Process, Risk, Control, Issues and Remediation, Perspectives, Assessment, and System Administration. Each duty roles includes the set of privileges needed to perform a certain aspect of work for a specific object, such as creating controls, managing controls, viewing controls, reviewing control changes, approving control changes, and other activities specific to an object.

Seeded duty roles are available; you are strongly recommended to use them. However, you may find that delivered duty roles do not align with how your organization segregates work responsibilities, or have functionality you do not wish to use.

- Review the delivered duty roles. You cannot change the seeded duty roles. If you need to make changes, create a new duty role by copying a delivered one, and then removing functionality from, or adding it to, the copy.

  For example, the Review Control Assessment seeded duty role includes the privilege to add attachments to completed controls during review. This may be something your organization does not allow the Control Assessment Reviewer to do. To remove this privilege, make a copy of the Review Control Assessment duty role, give it a new name, and remove this privilege from the new duty role.

- Construct duty roles in a way that aligns the tasks a user performs in a job. A user may perform multiple tasks that cross into different areas of the application. It is best to keep these tasks grouped into separate duty roles and then combine them in the job duty role.

  For example, the Control Manager needs the ability to administer controls and issues. It is better to have two duty roles, one for Control Administration and the other for Issue Administration, than to have one duty role that combines the two sets of tasks together.

  Keep this in mind as you define new duty roles, since this will provide you with the most reusability of duty roles. The delivered duty roles were created following this practice.

Constructing Data Roles

The data role defines which set of data the user has access to within the application. The system matches on the criteria for all the data roles within each user's job roles to determine the set of data to which the user has access. As covered in "Security Components" (page 7-1), two types of data role are delivered: primary data roles that include module, state, and state action, and composite data roles that reference a set of primary data roles to form the basic data access needed for a job role.

- Each primary data role is intended to be referenced by many composite data roles, depending on what actions are needed. You should not need to create pri-

mary data roles with module, state, and state action, but simply reference the delivered primary data roles.

- The application is delivered with primary data roles for all the standard objects within the module template, but without the Module filter. For a custom module, include the Module filter in the custom data roles. Refer to “Security for a New EGRCM Module” (page 7-20).
- A seeded composite data role exists for each seeded job duty role. Composite data roles have the same name as the job duty role, with the prefix *Data Role*. Each composite data role contains references to all the primary data roles that supply access to data required for the job.
- Data roles are extremely powerful in that, by their very construct, they define the degree of security to be implemented for all the duty roles (privileges) they are coupled with in the job role definition.

As delivered, the Financial Governance module does not have perspectives. This means that until you introduce perspectives into the module, access is determined only by whether a user has been granted the functional privilege and has access to the module.

- As you plan perspectives for your module, keep in mind that they are the means for segregating the data sets to which users have access. If you want only certain users to have access to a subset of operational data, define perspectives and include perspective filters in the composite data roles.
- First you must define the perspective. The values within the perspective are what will be associated to the application data. These same values are included within the data role. Their perspective must be defined with all its values before you can build the perspective data roles. Through the use of a perspective data role and associating perspective values to the operational data, you indicate the data to which each user has access. See “Module Perspectives” (page 1-9) and the “Perspective Management” chapter of the *EGRCM User Guide*.
- Perspectives are hierarchical. Within a data role, you can grant access to all data descending from a level of the hierarchy, by selecting that level within the hierarchy and selecting an Include Children option. This can reduce maintenance of the data role, since a filter defined this way does not have to change when new subordinate values are entered in the hierarchy.

  For example, an Organization perspective may be defined as follows:

  You can define roles that provide access to data at any level of the hierarchy, or to specific values:

  – For all data within the hierarchy, select ABC Corp and specify Includes Children.

  - For all data for a specific value and its subordinates (hierarchical branch), select a parent value and specify Include Children. If, in this example, your parent value is Division2, the role would grant access to data associated with Division2, Department1, Department2, Region1 and Region2 and all the values contained within the subfolders Region1 and Region2
  - For data only within a specific value, select that value, but do not specify Include Children. If you select a value that does have children, you are granting access only to the data associated with the value, and not to its children.

    For example, if you select Division2 but do not specify Include Children, then the role does not have access to data for Region1, Region 2, Department1, or Department2.

- To introduce data-level security, create a custom perspective data role with the appropriate perspective filters, and then reference the appropriate composite data role. If you use this technique, the system interjects the perspective filter into each primary data role included in the composite.

  Consider the perspective hierarchy illustrated on page 7-11. Each of the three divisions has its own Control Manager, and each manager is to have access only to controls within his division.

  To accomplish this, define three custom perspective data roles, one for each of the three divisions:

  - In each role, create a filter that sets the Organization perspective equal to one of the Division values — Division1 for a role called Control Manager Division 1 Data Role, Division2 for a role called Control Manager Division 2 Data Role, and Division3 for a role called Control Manager Division 3 Data Role.
  - In all three roles, create a filter that sets the Data Role attribute equal to Control Manager Data Role. This provides access to data defined by the seeded Control Manager composite data role.

  It's strongly recommended that the custom perspective data role reference a seeded composite data role. The custom perspective data role will automatically include any changes introduced to the seeded content in subsequent patches or releases.

- If a role includes more than one perspective value, it may treat those values with AND or OR logic, depending on how the role is configured. When values are combined in one filter, OR logic applies. For example, if a role contains one perspective filter that sets Organization equal to "Division1,Division2" the role grants access to all controls associated with either Division1 or Division2 (or both).

  When values are specified in distinct filters, however, AND logic applies. If, for example, a role contains two perspective filters, one sets Organization equal to "Division1" and the other sets Organization equal to "Division2," then the role grants access only to controls that have both Division1 and Division2 as the value for the Organization perspective.

- When a job role includes several data roles based on perspectives, those perspectives are joined by OR logic. This is desirable when a user requires access to objects associated with any of multiple perspective values — for example, controls for

which the value of a perspective called Manufacturing Region is North America or controls for which the value of a perspective called Sales Region is North America. (This returns a broader set of data than a single data role specifying data that meets both conditions.) So to expand the breadth of a job role, include multiple perspective data roles within it.

- During the initial phases of an implementation, it's recommended that you start with broader security access and over time, as you understand how the various security components of the application function, add granularity where necessary.

State Action

The state of an object identifies where it is within its life cycle. As activities are performed on an object, its state changes. Activities include updating values and submitting the change for review and approval, rejecting or approving the change, marking the remediation of an issue complete, closing an issue, and so forth.

The actions that can be performed against an object are determined by its state. Not all actions or activities are appropriate when an object is in a given state. This is controlled through the inclusion of the state within the primary data role. Duty roles identify specific sets of functional access and actions (privileges) a job role is granted. The state within the primary data role identifies which state the object must be in for this functional access and set of actions to be available.

The following tables list states appropriate to EGRCM objects, and actions appropriate to each state. Refer to these tables as you define custom primary data roles.

Make a note of the set of states that are appropriate for an action. When defining new primary data roles, you must include the correct state action for the appropriate entity so that this functionality is available only when the object is in the state identified by the data role.

Note: The application is seeded with a complete set of primary data roles for all objects, so it is highly unlikely that you will have to create a primary data role or a composite data role.

Risk and Risk Objects A–J, Event, Consequence, Control and Control Objects A–J, Process, Base Object A–F, Perspective, Assessment Template, Assessment Plan, and Survey Template

State	Description
New	Created and saved
In Edit	Changes made and saved, but not submitted
In Review	Submitted and awaiting review
Awaiting Approval	Review completed and awaiting approval
Additional Information in Review	In review, and the reviewer has asked for more information
Additional Information in Approval	Awaiting approval, and the approver has asked for more information
Rejected	Rejected during either review or approval
Approved	Approved

Assessment Result

State	Description
New	New assessment available for assessor to complete
In Edit	Changes made and saved, but not submitted
In Review	Completed assessment is submitted and awaits review
Awaiting Approval	Review completed and awaiting approval
Additional Information in Review	In review, and the reviewer has asked for more information
Additional Information in Approval	Awaiting approval, and the approver has asked for more information
Rejected	Rejected during either review or approval
Approved	Approved

Risk Analysis and Risk Evaluation

State	Description
In Edit	Active analysis or evaluation available to be completed
Complete	Analysis or evaluation results are completed

Issue

State	Description
New	Created and saved
Reported	Submitted for validation
In Edit	Changes made and saved, but not yet submitted
In Review	Submitted change is available for review
Awaiting Approval	Review completed and awaiting approval
Additional Information in Review	In review, and the reviewer has asked for more information
Additional Information in Approval	Awaiting approval, and the reviewer has asked for more information
Rejected	Rejected during either review or approval
Approved	Approved
Closed in Review	Issue is closed and is in review
Closed Approve	Review is completed for a closed issue, which awaits approval
Closed Additional Information in Review	A closed issue is in review, and the reviewer has asked for more information
Closed Additional Information in Approval	A closed issue awaits approval, and the approver has asked for more information

Remediation Plan

State	Description
New	Created and saved
In Edit	Changes made and saved, but not yet submitted
In Review	Submitted change is available for review
Awaiting Approval	Review completed and awaiting approval
Additional Information in Review	In review, and the reviewer has asked for more information
Additional Information in Approval	Awaiting approval, and the reviewer has asked for more information

State	Description
Rejected	Rejected during either review or approval
Approved	Approved
Completed Review	Remediation is completed and is in review
Completed Approve	Review completed for a completed remediation, which awaits approval
Completed Additional Information in Review	A completed remediation is in review, and the reviewer has asked for more information
Completed Additional Information in Approval	A completed remediation awaits approval, and the approver has asked for more information

Proposed Risk

State	Description
New	Created and saved
In Edit	Changes made and saved, but not yet submitted
Reported	Submitted for validation
Rejected	Rejected during validation

Assessment

State	Description
New	Created and saved
Active	Active assessment
Closed	Closed

Survey

State	Description
New	Created and saved
Open	Open and available for responders
Closed	Closed

Constructing Job Duty Roles

The job duty role is a type of job role that includes references only to duty roles. Isolating the functionality access from the data access provides reusability of the job duty role and makes it easier to construct new data access specific to job roles for the user community.

For example, the Control Manager Job Duty Role contains the following duty roles: Create New Control, Control Management, Create Issue for Control within Control Management, Create Issue for Control Assessments, Control Viewing, Control Assessment Result Viewing, and Control Reporting.

Instead of having to include these seven duty roles in each job role you create for specific data access, you reference only the job duty role, which has already formed the grouping.

The application is seeded with a set of job duty roles for the seeded job roles that are appropriate for the Financial Governance module. Each job duty role contains all the functional access needed for the job and defines “what can the user do” within the application.

- The UI allows you to construct job roles that include duty roles and data roles, but it is strongly recommended that you construct job duty roles to form groupings of duty roles. In this way you can reference the job duty role in job roles when you combine the functional and data access together. Each job duty role can be used in multiple job roles. This technique also makes it easier for you to make changes to the functional access, since changing a single job duty role applies the change to all users who perform a job against differing sets of data.
- Review the delivered job duty roles. Even if you did not create custom duty roles, you may find that the job duty role contains functionality that does not align with your compliance process. You cannot change seeded job duty roles directly. Create a new job duty role by making a copy of a delivered role and then removing duty roles from, or adding them to, the copy.

Constructing Job Roles

The job role brings both the functional access and the data access together to form precisely "what the user can do" to "which set of data." The application comes with seeded job roles that are appropriate for the Financial Governance module.

These seeded job roles are available for you to use to build out custom job roles you define to introduce data-level security. Each job role has a reference to the appropriate job duty role and the appropriate data role.

- Create a job role for each set of functional access and unique set of data access required for all the operational data secured by perspectives.

  Earlier, the "Constructing Data Roles" section presented a sample Organization perspective (page 7-11) that established three divisions. The section discussed creating three custom perspective data roles (page 7-12), each of which granted access to control-management data for one of the divisions.

  Using those data roles, you can create job roles, one for each division. All three job roles would cite the Control Manager Job Duty Role, which encompasses all the functionality a user requires to serve as a Control Manager. Each of the three job roles would also cite one of the custom perspective data roles configured to provide access to the data for each division: Control Manager Division 1 Data Role, Control Manager Division 2 Data Role, and Control Manager Division 3 Data Role.

  Note: It's recommended that you include the perspective value within the job role name so that you can easily identify the data that a given job role uses, and to make it easier to locate job roles when assigning them to users.

- A job role can reference other job roles. This type of job role can contain only other job roles, and acts as a way to group a set of job roles needed for a specific user type.

  For example, you can create a job role named Basic Financial Governance Access Job Role; it might contain two other job roles called GRC User Job Role and Financial Governance Job Role. Then you could grant only the Basic Financial Governance Access Job Role, rather than the two separate roles, to any user who would qualify to have both those roles.

Perspective Matching Based on the Data Roles within the Job Role

When an object contains perspectives, a user's data roles must have at least one of the object's perspective values in order for the user to have access to the object.

When a job role contains data roles with perspectives, the system compares all the perspective values within the data role against those in the object.

The data role drives which perspectives to match on for the user:

- For the user to have access to the data, at least one value for each perspective filter within the data role must match a perspective value associated with the object.

  For example, assume both the Financial Governance and IT Governance modules identify an Accounts Payable process, with Organization perspective values of Division1 and Division2. User1 has a data role that permits viewing of processes for the Financial Governance module for Division1. User1 can view the Accounts Payable process, since Financial Governance and Division1 match values for Module and Organization.

- If the data does not have a value for a perspective within the data role, then it cannot be matched on.

  For example, User1 has a job role that includes a data role that allows users to view the Process object. The data role for this job role contains the criteria that Module = Financial Governance, Organization = Division1, and Major Process = Procure to Pay.

  The Accounts Payable process is related to the Organization value of Division1, but Major Process is not completed.

  User1 does not have access to Accounts Payable, since the data role for this job role contains both the Organization and Major Process perspectives. The criteria for Major Process cannot be matched since no value is specified on the object.

Manage Users

The basic security principle is that a user does not have access to application functionality unless it is specifically granted to the user.

- All users must have basic access to EGRCM that is provided by the seeded GRC User Job Role. This job role includes only the basic privilege to log into the application and see the Welcome dashboard. Beyond this, each user's security profile must be updated to grant privileges to perform other activities, and to define precisely the application data to which the user has access.

  Note: The user has access to the operational data that is not secured by a perspective based solely on functional access. Some operational data is not secured by perspectives, such as survey management objects and assessment management objects, and access to this data is based on the functional access. Likewise, if an object that does support perspectives is defined without any perspectives, that object is not secured by data access and any user that has the functional access to the object will have access to it.

For example, the Order to Cash process is defined without any perspectives associated to it. All users who have a data role to view the process object in the Approved state regardless of any of the perspective filters contained in their data roles will be able to view the Order to Cash process.

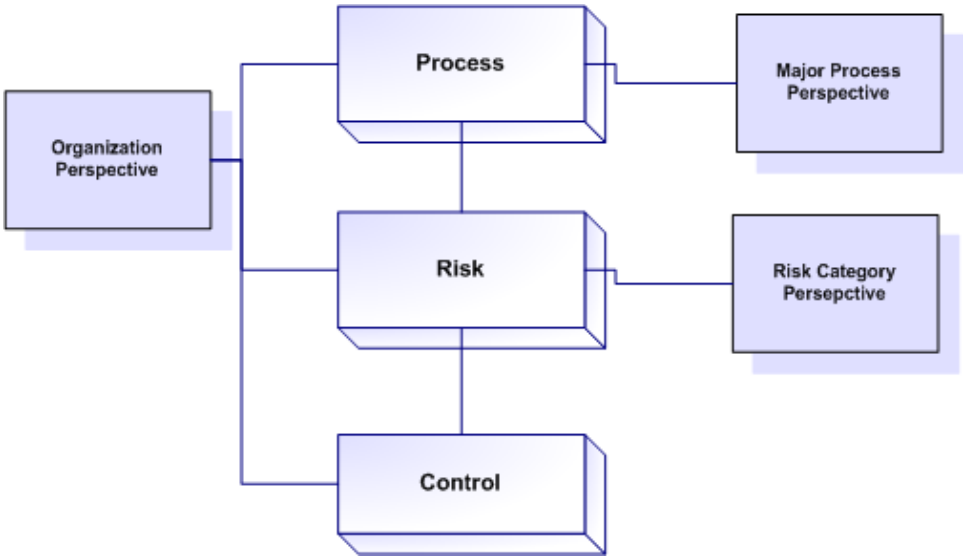
- To have the Financial Governance module displayed within the Navigator, the user must have the Financial Governance Module Job Role.
- Select all other appropriate job roles for each user.
- Each user must have a unique email address. Users cannot share an email address.
- A user assigned multiple job roles has access that is the combination of all those job roles.

  For example, if the user has the job roles for performing control maintenance and issue maintenance for the Financial Governance module, then within the Navigator for Financial Governance, both the Control Management and Issue Management entries are available.

Define a User with Access to All Operational Data

It's recommended that you define at least one "Super User" — a user who can view all operational data. To do this, create data roles for perspectives associated to the objects. Include a filter with the Includes Children condition, and select the root value. Include this data role with the viewing job duty role for the object.

For example, assume you configured the Financial Governance module to have the following perspectives:



The Organization perspective is associated with all three objects in this module, so this perspective can be used to define the data roles.

1. Create three custom perspective data roles: All Processes Viewer Data Role, All Risks Viewer Data Role, and All Controls Viewer Data role:
   - All three roles contain a filter that sets the Organization perspective equal to Organization (its root value), and specifies the Includes Children condition.

- Each contains a filter that sets the data role equal to the seeded viewer role for its object: Process Viewer Data Role, Risk Viewer Data Role, and Control Viewer Data Role, respectively.

2. Define three custom job roles: All Processes Viewer Job Role, All Risks Viewer Job Role, and All Controls Viewer Job Role:
   - All Processes Viewer Job Role includes the All Processes Viewer Data Role created in step 1 and the seeded Process Viewer Job Duty Role.
   - All Risks Viewer Job Role includes the All Risks Viewer Data Role created in step 1 and the seeded Risk Viewer Job Duty Role.
   - All Controls Viewer Job Role includes the All Controls Viewer Data Role created in step 1 and the seeded Control Viewer Job Duty Role.
3. Assign the new custom job roles to a user.

Access to Issues within Issue Management

Access to issue data is driven by the object the issue is raised against. Therefore issue security access combines issue privileges and data access to objects within a module. Consider these points while defining users' job roles for Issue Management:

- To be granted access to Issue Management, a user have a job role that cites a job duty role with at least one of these privileges: View Issues, Create Issue, Edit Issue, Validate Issue, Close Issue, Review Issue Changes, Approve Issue Changes.
- Within Issue Management, the system determines the issues to which a user has access based on the object each issue is raised against and whether the user has access to that object. That means the user's other job roles determine the issues to which the user has access.

  For example, a control called Segregation of Duties for Division1 within the Financial Governance module has an issue raised against it.

  – User1 has an Issue Manager Job Role that includes a job duty role containing the View Issues and Validate Issue privileges and data roles to edit issues when in the Reported, Approved, In Edit, and Rejected states for the Financial Governance Module.

  – User1 also has a Control Manager Job Role that includes a job duty role containing privileges to create, edit, and view the control object and a data role to view the control object for the Financial Governance module when the state is equal to Approved.

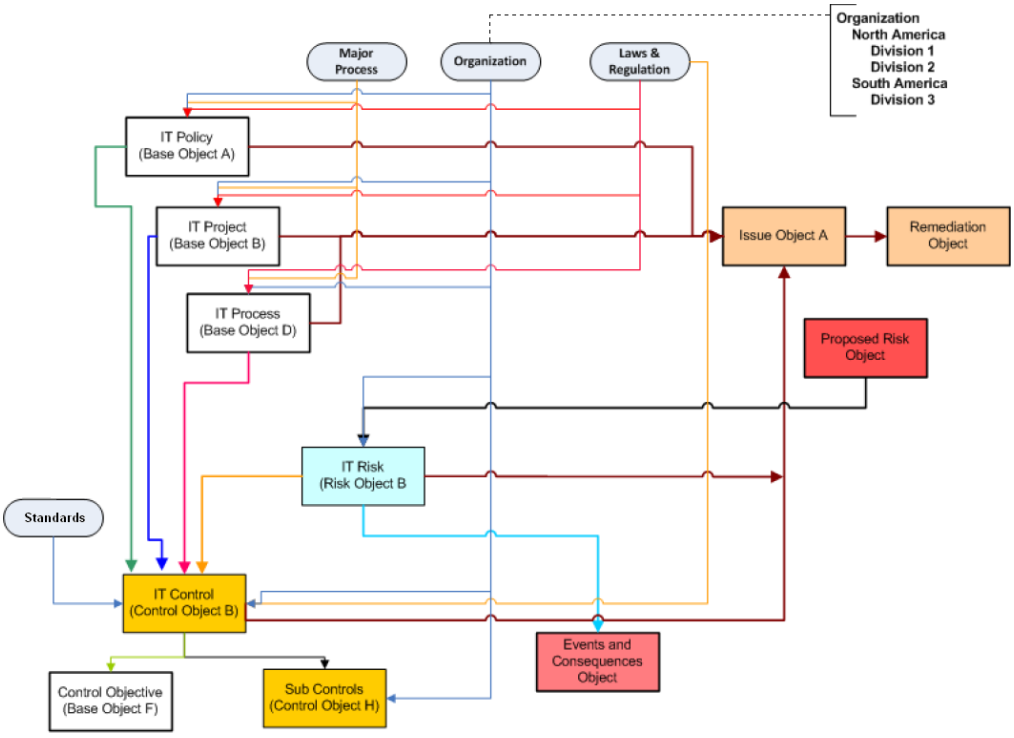
  – Upon navigating to Issue Management within the Financial Governance module, User1 sees the issue raised against the Segregation of Duties control because of the privileges and data access granted by the Control Manager Job Role and the Issue Manager Job Role.

  – The system also generates a worklist entry for User1 to validate the submitted issue for the Segregation of Duties control, because User1 is granted the Edit Issue data role when the state of the issue is Reported within the Issue Manager Job Role.

Security for a New EGRCM Module

If you configure a new module as discussed in the "Module Management" chapter (beginning on page 4-1), you must define new security roles for the objects configured within the new module.

First, review the module definition and identify all the template objects being used. The following might be used for an IT Governance module:



Based on this diagram, the new IT Governance module includes:

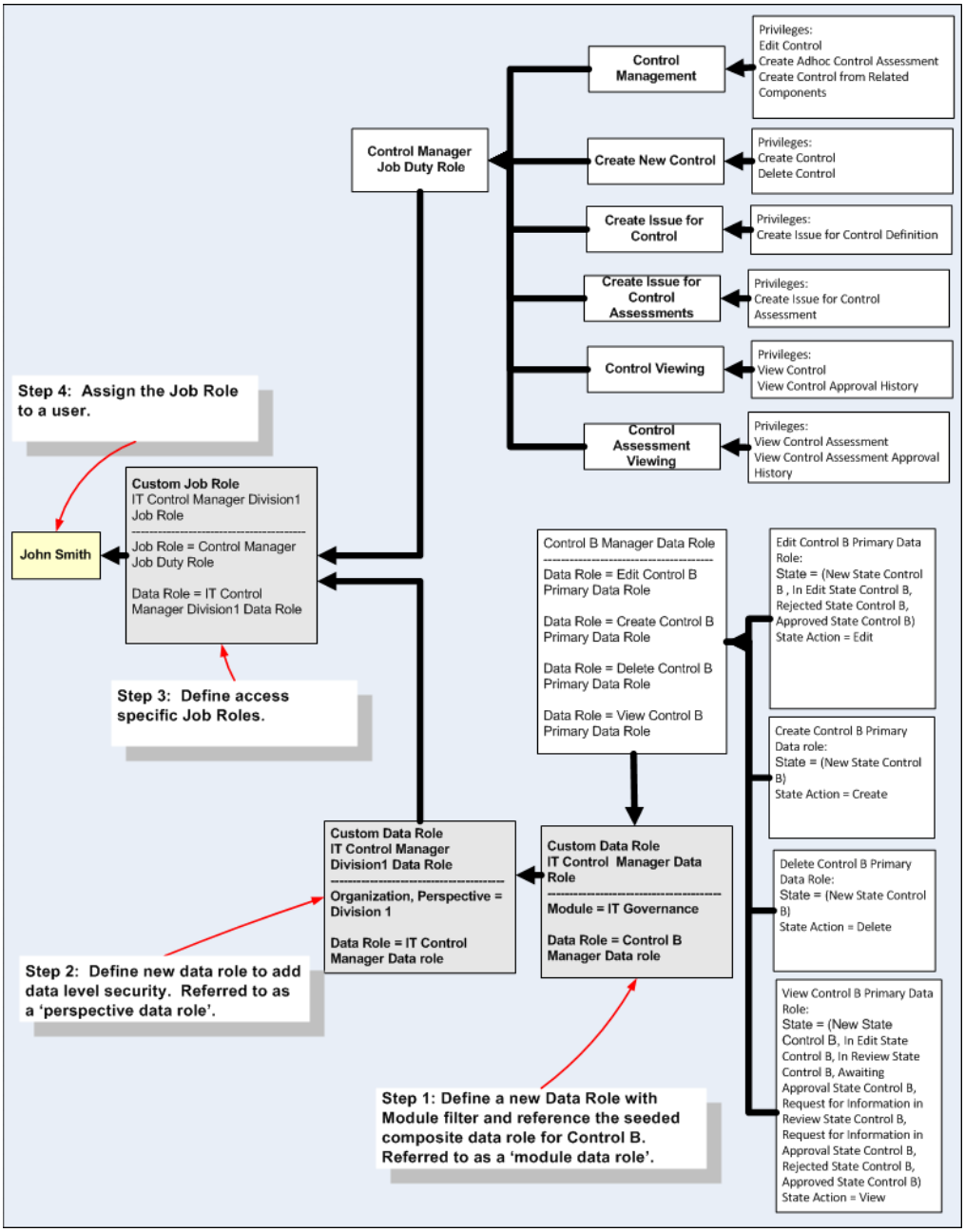
Object	Relabel	Module Specific
Base Object A	IT Policy	×
Base Object B	IT Project	×
Base Object D	IT Process	×
Risk Object B	IT Risk	×
Control Object B	IT Control	×
Control Object H	Sub Control	×
Base Object F	Control Objective	×
Event	Event	
Consequence	Consequence	
Proposed Risk	Proposed Risk	
Issue Object A	Issue	×
Remediation Plan	Remediation Plan	

Next, identify the types of job roles you need for this new module and the type of functional access each job role needs. You can use the seeded duty and job duty roles for the functional access if these meet your business requirements. If not, see "Constructing Duty Roles" and "Constructing Job Duty Roles" (pages 7-10 and 7-15).

Then complete the following steps:

1. Define a data role for each seeded composite data role for the standard objects in the new module and include the module filter. This is also referred to as the "module data role." See "Define Data Roles for the New Module" (page 7-22).
2. Define perspective data roles for data-level security as needed. See "Define Perspective Data Roles for Data Level Security" (page 7-23).
3. Define new job roles. See "Define New Job Roles" (page 7-23).
4. Assign the new job roles to users.

The following diagram illustrates the steps to define the IT Control Manager Division 1 Job Role for the IT Governance module. The shaded boxes represent roles that are needed for the custom module; the unshaded boxes are seeded roles.



Define Data Roles for the New Module

The application is delivered with a complete set of primary and composite data roles for all the objects within the module template.

- The application is seeded with primary data roles for standard objects in the module template. For each, the object name is contained within the role name, and each references the specific state for the standard object the primary data role serves. The roles do not contain the module filter. For example:

Name: Edit Control Object B Primary Data Role

Description: Data access criteria to edit Control Object B data

Filter Name	Object	Attribute	Condition	Value	Include/Exclude
States	Data Attributes	State	Equals	New State Control Object B, In Edit State Control Object B, Rejected State Control Object B, Approved State Control Object B	Include
Action	Data Attributes	Action	Equals	Edit	Include

- The seeded composite data roles for the standard objects are defined similarly to those that support the seeded job roles for Financial Governance. These composites form groupings of data access against each of the standard objects. For example:

Name: Control Object B Manager Data Role

Description: Composite data role for access to edit Control Object B data

Filter Name	Object	Attribute	Condition	Data Role	Include/Exclude
Edit	Data Attributes	Data Role	Equals	Edit Control Object B Primary Data Role	Include
View	Data Attributes	Data Role	Equals	View Control Object B Primary Data Role	Include
View Assessment	Data Attributes	Data Role	Equals	View Control Object B Operational Assessment Results Primary Data Role	Include
View Design Review	Data Attributes	Data Role	Equals	View Control Object B Design Review Assessment Results Primary Data Role	Include
View Audit Test	Data Attributes	Data Role	Equals	View Control Object B Audit Test Assessment Results Primary Data Role	Include
View Certification	Data Attributes	Data Role	Equals	View Control Object B Certification Assessment Results Primary Data Role	Include
Create	Data Attributes	Data Role	Equals	Create Control Object B Primary Data Role	Include
Delete	Data Attributes	Data Role	Equals	Delete Control Object B Primary Data Role	Include

Because primary data roles for standard objects do not include module, you must define custom "module data roles." Each of these associates the new module with the seeded composite data role for one of the objects selected for the new module.

For example, the sample IT Governance module uses Control Object B for its control object. You might create this role:

Name: IT Control Manager Data Role

Description: Maintain IT Control data access

Filter Name	Object	Attribute	Condition	Value	Include/Exclude
Module	Data Attributes	Module	Equals	IT Governance	Include
Data Role	Data Attributes	Data Role	Equals	Control Object B Manager Data Role	Include

Define Perspective Data Roles for Data-Level Security

To introduce data-level security for the new module, follow a process very similar to the one used for the Financial Governance module. Create custom data roles, each of which contains at least one filter that specifies at least one perspective value to be applied to an object, and another filter which in this case references the module data role for that object (as created in "Define Data Roles for the New Module," above).

For example, suppose (once again) the Organization perspective includes values that divide a company into divisions, and one of these values is Division1. In the IT Governance module, you want to provide a Control Manager with access only to controls in Division1. Create a role (called, for instance, IT Control Manager Division 1 Data Role) that includes two filters:

- A filter called Division1 sets the Organization perspective equal to Division1.
- A filter called Control Manager sets the data role equal to the IT Control Manager Data Role created (above) to apply control-management data access to the IT Governance module.

The system joins the perspective-filter criterion with all the filter criteria introduced in the module data role, as well as within each of the primary data roles contained in the seeded Control Object B Manager Data Role.

The system uses AND logic to join the perspective filter with other data role criteria, and so grants access to controls for which all of the following are true:

- The perspective value associated to a control must equal Division1 (the condition of the Division1 filter).
- The control must exist in the IT Governance module (a condition of the IT Control Manager Data Role).
- The control must be of the object type Control Object B and must be in one of the following state/action combinations (a condition of the IT Control Manager Data Role, because each combination is defined in one of the primary data roles that belong to the Control Object B Manager Data Role, which in turn is a component of the IT Control Manager Data Role).
  - Control State equals any of New State Control, In Edit Stat Control, Rejected State Control, or Approved State Control AND Action equals Edit.
  - Control State equals New State Control AND Action equals Delete.
  - Control State equals any of New State Control, In Edit State Control, In Review State Control, Awaiting Approval State Control, Request for Information in Review State Control, Request for Information in Approval State Control, Rejected State Control, or Approved State Control, AND Action equals View.

Define New Job Roles

Create new job roles for the new module as described in "Constructing Job Roles" (page 7-16). The only difference is that these job roles reference the new job duty role and data roles created for the new module.

Create Job Roles for Issue and Remediation Plan for a Custom Module

Job roles for issue and remediation plans for a custom module are handled slightly differently than for other standard objects.

Access to issues is based on the user having the appropriate functional access to the Issue object and having data access to the Issue object and data access to the object the issue is against.

There is only one Remediation Plan object, and it is not module- or object-specific. Access to Remediation Plan is based on having the appropriate functional access to the Remediation Plan object and having data access to the Remediation object.

When defining a new Issue Job Role for the custom module, it is necessary to add in the module filter as described in "Define Data Roles for the New Module" (page 7-22). However, you will never build a perspective data role for the Issue object; issues do not have perspectives.

For example, an IT Issue Manager Data Role might contain two filters:

- A filter called Module sets the module equal to IT Governance.
- A filter called Data Role sets the role equal to the seeded Issue Object A Manager Data Role.

The issues to which a user actually has access are based on the object against which the issues are logged. A user has access only to issues within Issue Management for objects the user can access in other work areas. So a user who is an Issue Manager is able to edit and maintain issues only for objects to which the user has access. Therefore to define new issue job roles for a custom module:

- Define the module data role to grant access to the Issue object in the new module.
- Define the module-specific job role that references the new module data role.
- For access to remediation plans, use the seeded job roles. There is only one Remediation Plan object, which spans all modules. Users with access to Remediation Plan data have access to all remediation plans within the application.

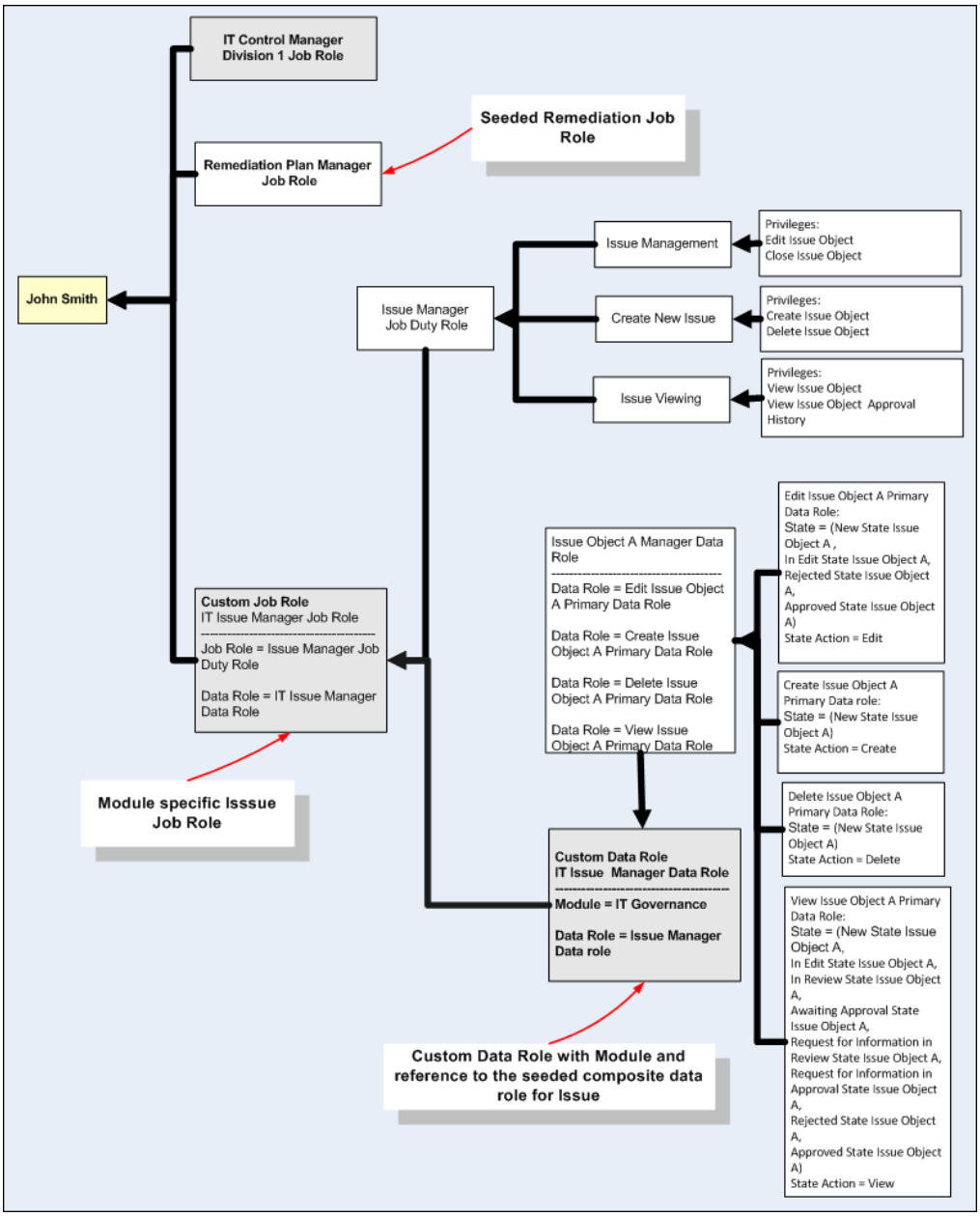
This diagram on page 7-25 shows Issue and Remediation Plan security for a custom module.

Security for Event, Consequence, and Proposed Risk

Like Remediation Plan, there is only one object for each of Event, Consequence, and Proposed Risk. This means there is no need for custom security roles to grant a user access to these objects; the seeded roles can be used.

Event, Consequence, and Proposed Risk are also not module-specific. Regardless of the module from which a user navigates into Risk Management, the user sees all instances.

These components do not have perspectives, so there is no data-level security for them.



Impact of Changing a Perspective Used in Data Roles

Over time it may be necessary to make changes to perspectives used for data-level security. It is important to understand if a change will impact security, and how.

Change	Impact
Changing the name, description, or status of a value within the perspective hierarchy	No
Moving a value to a new position within the hierarchy so that it retains its original parent value	No

Change	Impact
Moving a value to a new position in the hierarchy so that it changes its parent value	Yes For users with a data role in which a perspective filter is set to equal this value, there is no impact. If a data role includes a perspective filter that refers to the original parent and uses the Includes Children condition, users assigned the role no longer have access to objects associated to the value that was moved. If a data role includes a perspective filter that refers to the new parent and uses the Includes Children condition, users assigned the role now have access to objects associated to the value that was moved.
Removing a value from the hierarchy	Yes Any object associated with the perspective value that was removed will no longer be accessible. The Unassigned Perspective Values security report will report these objects. When you find it necessary to remove a value from a perspective hierarchy, first change all objects that are associated with that value to a new perspective value and update users' data roles accordingly. If that new value does not already exist within the perspective hierarchy: • Update the perspective hierarchy with the new value. • Update objects associated with the value to be removed to the new perspective value. • If necessary, update the data roles that referenced the value to be removed to the new value or a parent value with Includes Children. • Update the perspective hierarchy to remove the perspective value.
Changing the status of the perspective hierarchy to Inactive	Yes Any object associated with the perspective hierarchy is no longer accessible. This change requires multiple steps. If this perspective hierarchy is to be replaced by a newly created one: • Define the new hierarchy first. • Define new data roles for this hierarchy or update existing data roles. If existing data roles are updated, users whose job roles reference the changed data roles will have new access. If a new perspective hierarchy is not needed, but an existing perspective hierarchy will be used: • If necessary, update the existing perspective hierarchy with values. • If necessary, define new data roles for the new values or update existing data roles for the new values. In either case: • Optionally, assign the new data roles to the appropriate users by either creating new job roles or including the new data roles in existing job roles. • Change the objects associated to values in the perspective hierarchy to be retired to the new perspective hierarchy. • Update the perspective hierarchy status to Inactive. • Optionally, update the status to Inactive for the data roles for the inactive perspective hierarchy. • Optionally, remove inactive data roles from the job roles.

8

Preparing for a Production Environment

Typically an IT organization develops a specific release process, which is managed internally. It is common to see a variety of release approaches. However, a number of common deployment tiers are designated in the release process. The following are common milestones that can be found in an application release process:

- Development: A development server (sandbox) for installing the application, configuring it, and preparing and loading legacy data into it. It is strongly recommended that a current snapshot be taken of the environment before any significant change is applied to the development instance, such as importing legacy data or installing a patch.
- Staging/Preproduction: A mirror image of the production environment. Users can complete comprehensive testing prior to production. At this point, if critical issues have been identified, the environment's database can be rolled back to the prior snapshot.

  Additional common release tiers could include:

  – Integration: Developer testing if any side effects have occurred.

  – Test/QA: For functional, performance testing, quality assurance (data integrity, security, and general configuration).

  – UAT: User acceptance testing.
- Production/Live: Servers are available to the end user.

Each of these milestones is broken down into phases. Each phase provides a sequential order of recommended steps to follow during the implementation of an EGRCM environment.

Phase 1: Development (Initial Sandbox/CRP)

1. Install and patch to latest level.
2. Take a backup of the instance that does not include any data.
3. Enter in test data for training, Conference Room Pilot (CRP), and User Acceptance Test (UAT).
4. Refine import file and test import.

5. Finalize operational and setup data import file for preproduction setup.
6. Restore from "Gold" backup when new releases are available or for iterations of import-file testing.
7. Repeat steps 1–6 as necessary.
8. Patch environment to latest release level (or apply as fresh install with new schema).
9. Take a Gold backup of the instance that does not include any data.
10. Put together preproduction setup documentation (script specific to your setups).
11. Phase 1 conclusion. This means your import file is close to being completed and you have determined how you want to set up your UDAs, perspectives, and security definitions (i.e., duty, data, and job role constructs and whom they are to be assigned to).

Phase 2: Staging/Preproduction Setup

1. Restore to a clean environment.
2. Upgrade environment to latest release (or apply as fresh install with new schema).
3. Take a Gold backup of the instance that does not include any data.
4. Input initial setups:
   - Configuration options
   - UDAs
   - Lookup values
5. Import operational and setup data. Note: The import file may undergo additional modifications based on UAT.
6. Input next setups:
   - Perspective hierarchies
   - Perspective/object association
   - Data, duty, and job roles
7. Take a Gold backup with data and setups. As a precaution, however, do not blow away the Gold backup from step 3.
8. Perform UAT.
9. Determine if setups and import data are appropriate (i.e., they pass) from UAT experience. If they do not pass, restore the Gold backup from step 3 and repeat steps 4–7 (step 8 is optional). If they do pass, restore the Gold backup from step 7 and continue at the next step.
10. Patch to the latest release if applicable.

11. Take Gold backup with data and setups.
12. Test and validate preproduction as necessary.
13. Restore Gold backup from step 11 and apply all necessary patches. Repeat until step 12 is satisfied.
14. Restore Gold backup from step 11 and apply all necessary patches.
15. Take final preproduction Gold backup.
16. Install into production environment and migrate the production database from the Gold backup.

Phase 3: Production/Live Maintenance

1. Clone production database.
2. Deploy clone to Development and Test instances.
3. Apply latest release to Development.
4. Test the upgrade and sign off.
5. Apply latest release to Test instance.
6. Test upgrade and sign off.
7. Apply latest release to Production instance.

Periodic Gold Backup Update

User passwords expire, so it is necessary to update the user password for the admin user within the Gold backup before that password expires.

By default, a password remains valid for 90 days (although you can change this value in an Elapsed Days Before Password Expires field on the Security tab of the Manage Application Configurations page). So as an example, if you use the default password-expiration value, you must update the admin user password for the Gold backup before 90 days pass, then generate a new Gold backup. This way it is possible to sign in as the admin user and reset other user passwords. If this is not done, when the backup is restored, the system detects that the admin password has expired, and the admin user is locked out of the application like any other user.

1. Every 89 days — or a number of days less than your password-expiration setting — restore the Gold backup created in step 15 of "Phase 2: Staging/ Preproduction Setup."
2. Update the password for the admin user.
3. Take a new Gold backup.

Note: If the admin user password does expire in the Gold backup, contact Oracle support for assistance.

Installing EGRCM Patch Sets

During the implementation of a GRC environment, sequential patches may become available. The following provides scenarios and approaches you can take.

Option 1:

1. Fresh install, which replaces the application schema with a new empty one.
2. Take backup to create a new Gold image.
3. Release as Development to functional team for additional testing.

Option 2

1. Restore Gold image.
2. Apply patch.
3. Take backup to create new Gold image.
4. Release as Development to functional team for additional testing.
5. Back up the instance prior to the release. The key is not to include any of the test data (i.e., configuration, records, and transactions).

A

Appendix

This appendix provides additional information about EGRCM, such as trouble-shooting tips, use cases, and lists of delivered objects and pattern mappings.

Troubleshooting Import Data

The import process may result in data-validation errors, duplicate-name errors, or SQL errors. The following sections provide advice on resolving these.

Understanding Import Error Messages

The import process may detect data inconsistencies within the import template. In this case, the system alerts you with an error message after you have started the import. The message helps you determine the cause of the problem. If you have many validation errors, export to Excel to make it easier to work through them.

The following is a sampling of errors you may encounter:

- Entity referenced by the attribute is not found (entity referenced, attribute name, attribute value, sheet name, row number) Control, CONTROL_ID, 1, TreatmentControl, 3
- Entity referenced by the attribute is not found (entity referenced, attribute name, attribute value, sheet name, row number) Event, EVENT_ID, 5, RiskEvent, 7
- Entity referenced by the attribute is not found (entity referenced, attribute name, attribute value, sheet name, row number) Control, CONTROL_ID, 1, RiskControl, 3
- Entity referenced by the attribute is not found (entity referenced, attribute name, attribute value, sheet name, row number) Control, PARENT_CONTROL_ID, 2, RiskControl, 3
- Attribute given is not defined (attribute name, sheet name) UDA_uda 1 for Process, Process
- Attribute given is not defined (attribute name, sheet name) UDA_uda 2 for PerspectiveItem, PerspectiveItem
- Attribute value given is not in the valid list of values (attribute name, attribute type, sheet name, row number) STATE_CODE, aaa, PerspectiveItem, 4

- Wrong attribute type given for the attribute (attribute name, attribute type, sheet name, row number) UDA_uda 1 for PerspectiveItem, DateTime, PerspectiveItem, 5
- Wrong attribute type given for the attribute (attribute name, attribute type, sheet name, row number) RISK_ID, Number, ProcessRisk, 4
- Wrong attribute type given for the attribute (attribute name, attribute type, sheet name, row number) LIKELIHOOD_MODEL_ID, Number, Event, 7

Using the first error message in the preceding list as an example, you can generally interpret error messages as follows:

- The first part is the actual error — for example, "Entity referenced by the attribute is not found."
- Information following the actual error includes, in parentheses, labels describing the items involved in the error, followed by the actual items. For example:

  (entity referenced, attribute name, attribute value, sheet name, row number) Control, CONTROL_ID, 1, TreatmentControl, 3

  – entity referenced, Control: The problem occurred for the Control object.

  – attribute name, CONTROL_ID: The issue is with the value entered for CONTROL_ID.

  – attribute vale, 1: The Control ID value of 1 does not reference a valid control.

  – sheet name, TreatmentControl: The error is within the TreatmentControl tab of the import template.

  – row number, 3: The error is in the third row of data.

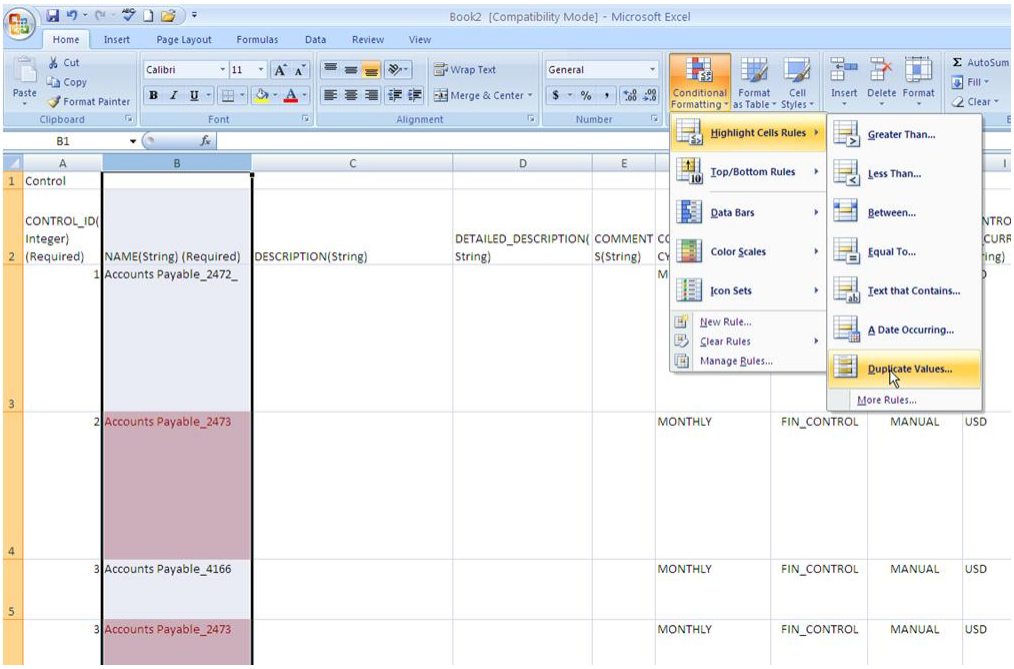
Using this error-message information, look at the TreatmentControl tab in the import template. Look at the third row of data (ignore the header rows). The value in CONTROL_ID (1) does not reference a control.

How to Find Duplicate Names

If you receive duplicate name errors, change the names so that they are unique within each worksheet.

If you are using Excel 2007, use conditional formatting to search for duplicate names:

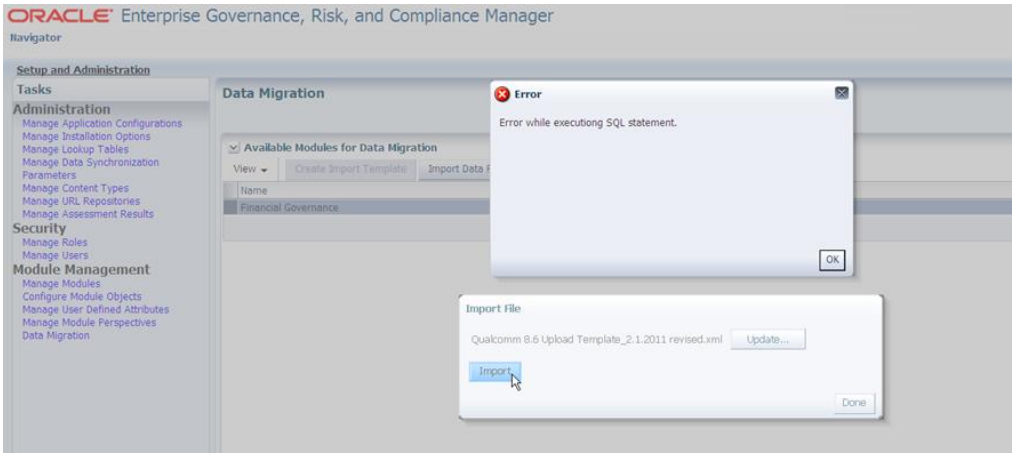
1. Select the column on the worksheet that contains the name.
2. Select Conditional Formatting > Highlight Cells Rules > Duplicate Values.
3. Select Duplicate, and select a highlight scheme. Duplicate names are then highlighted (see the illustration at the top of the next page).
4. Sort the worksheet on the Name column so that rows with duplicate names appear together.



5. Eliminate duplications. If you determine a duplicate name is actually a duplicate row in the worksheet and you remove it, be sure to remove also any references to this row ID in any associated worksheets.
6. After you have made the corrections, remove the conditional formatting.

SQL Error While the Import Runs

During the import process, you may encounter a SQL error.



To troubleshoot the error, ftp the grc.log from the following location on the host:

```
$<MW_HOME>/user_projects/domains/grc_domain/servers/AdminServer/
stage/grc863/grc863/grc/log
```

Open the grc.log in a text editor (such as WordPad), then search for "SQL statement" and check the corresponding timestamp before analysis.

The following is a sample error from the log:

```
2011-02-01 12:19:47,381 ERROR [el.Default (self-tuning)'] AbstractDaoSpr:515
Error while the execution of the SQL statement.
org.springframework.dao.DataIntegrityViolationException:
PreparedStatementCallback; SQL [INSERT INTO GRC_CTRL_ASSERTION (CONTROL_ID,
ASSERTION_CODE, EFFECTIVE_SEQUENCE, START_DATE, CREATION_DATE, CREATED_BY,
@ LAST_UPDATE_DATE, LAST_UPDATED_BY, LAST_UPDATE_LOGIN) VALUES (?, ?, ?, ?, ?, ?,
?, ?, ?)]; ORA-01400: cannot insert NULL into
("GRC863"."GRC_CTRL_ASSERTION"."ASSERTION_CODE")
; nested exception is java.sql.SQLIntegrityConstraintViolationException:
ORA-01400: cannot insert NULL into
("GRC863"."GRC_CTRL_ASSERTION"."ASSERTION_CODE")
```

Troubleshooting Access

If a user should have access to data but cannot see it, the problem is probably an incorrect data role.

- Review the perspective filter that is included in the user's data role. Does it reference the correct perspective and perspective value? Is the condition correct?
- Is the correct composite data role referenced for the user's job role?

List of Delivered Privileges

The following table contains all the seeded privileges within GRC. The table is organized by Navigator entry and activity, so all the privileges for a specific activity within the application are listed together. You cannot create new privileges. A privilege correlates to a specific object, action, or page within the application.

If a user receives an error message denying access to a page, does not see an action enabled on a page, or is missing a task list entry, it is most likely due to a missing privilege. Review this list of privileges to determine which one is missing from the user's duty role.

You may find it easier to work with this privilege table if you copy it and paste it into Excel.

Navigator Entry	Activity	Privilege Name
Control Management	Control Assessment	Create Control Adhoc Assessment
Control Management	Control Assessment	Create Issue for Control Assessment
Control Management	Control Assessment	Complete Control Assessment
Control Management	Control Assessment	Review Control Assessment
Control Management	Control Assessment	Add Attachments to a Completed Control Assessment
Control Management	Control Assessment	Approve Control Assessment
Control Management	Control Maintenance	Create Control
Control Management	Control Maintenance	Create Control from Related Components
Control Management	Control Maintenance	Edit Control
Control Management	Control Maintenance	Create Issue for Control Definition
Control Management	Control Maintenance	Review Control Changes
Control Management	Control Maintenance	Approve Control Changes

Navigator Entry	Activity	Privilege Name
Control Management	Control Maintenance	Delete Control
Control Management	Control Management	View Control
Control Management	Control Management	View Control Approval History
Control Management	Control Management	View Control Assessment Approval History
Control Management	Control Management	View Control Assessment Results
Financial Governance	Financial Governance	Display Financial Governance in the Navigator
GRC Tools	Assessment Maintenance	Create Assessment Template
GRC Tools	Assessment Maintenance	Delete Assessment Template
GRC Tools	Assessment Maintenance	Edit Assessment Template
GRC Tools	Assessment Maintenance	Review Assessment Template Changes
GRC Tools	Assessment Maintenance	Approve Assessment Template Changes
GRC Tools	Assessment Maintenance	Create Assessment Plan
GRC Tools	Assessment Maintenance	Delete Assessment Plan
GRC Tools	Assessment Maintenance	Edit Assessment Plan
GRC Tools	Assessment Maintenance	Review Assessment Plan Changes
GRC Tools	Assessment Maintenance	Approve Assessment Plan Changes
GRC Tools	Assessment Maintenance	Initiate Assessment
GRC Tools	Assessment Maintenance	Close Assessment
GRC Tools	Assessment Maintenance	Edit Assessment Due Date
GRC Tools	Assessment Management	View Assessment Template
GRC Tools	Assessment Management	View Template Approval History
GRC Tools	Assessment Management	View Assessment Plan
GRC Tools	Assessment Management	View Assessment Plan Approval History
GRC Tools	Assessment Management	View Assessment
GRC Tools	Assessment Management	Notify Participants of an Assessment
GRC Tools	Survey Maintenance	Create Question
GRC Tools	Survey Maintenance	Edit Question
GRC Tools	Survey Maintenance	Review Question Changes
GRC Tools	Survey Maintenance	Approve Question Changes
GRC Tools	Survey Maintenance	Create Question Choice Sets
GRC Tools	Survey Maintenance	Edit Question Choice Sets
GRC Tools	Survey Maintenance	Create Survey Template
GRC Tools	Survey Maintenance	Delete Survey Template
GRC Tools	Survey Maintenance	Edit Survey Template
GRC Tools	Survey Maintenance	Review Survey Template Changes
GRC Tools	Survey Maintenance	Approve Survey Template Changes
GRC Tools	Survey Maintenance	Create Survey
GRC Tools	Survey Maintenance	Edit Survey
GRC Tools	Survey Maintenance	Delete Survey
GRC Tools	Survey Management	View Survey Questions
GRC Tools	Survey Management	View Question Approval History
GRC Tools	Survey Management	View Question Choice Sets
GRC Tools	Survey Management	View Survey Template

Navigator Entry	Activity	Privilege Name
GRC Tools	Survey Management	View Survey Template Approval History
GRC Tools	Survey Management	View Surveys
GRC Tools	Survey Management	View Survey Responses
GRC Tools	Survey Management	Notify Survey Translators
Issue Management	Issue Maintenance	Create Issue
Issue Management	Issue Maintenance	Edit Issue
Issue Management	Issue Maintenance	Validate Issue
Issue Management	Issue Maintenance	Close Issue
Issue Management	Issue Maintenance	Review Issue Changes
Issue Management	Issue Maintenance	Approve Issue Changes
Issue Management	Issue Maintenance	Delete Issue
Issue Management	Issue Management	View Issues
Issue Management	Issue Management	View Issue Approval History
Issue Management	Issue Remediation Management	View Remediation Plan
Issue Management	Issue Remediation Management	View Remediation Plan Approval History
Issue Management	Remediation Plan Maintenance	Create Remediation Plan
Issue Management	Remediation Plan Maintenance	Edit Remediation Plan
Issue Management	Remediation Plan Maintenance	Complete Remediation Plan
Issue Management	Remediation Plan Maintenance	Complete Remediation Task
Issue Management	Remediation Plan Maintenance	Review Remediation Plan Changes
Issue Management	Remediation Plan Maintenance	Approve Remediation Plan Changes
Issue Management	Remediation Plan Maintenance	Delete Remediation Plan
Issue Management	Remediation Tasks	Create Remediation Task
Issue Management	Remediation Tasks	Edit Remediation Task
Perspective Management	Perspective Assessment	Create Perspective Hierarchy Adhoc Assessment
Perspective Management	Perspective Assessment	Create Issue for Perspective Assessment
Perspective Management	Perspective Assessment	Complete Perspective Assessment
Perspective Management	Perspective Hierarchy Maintenance	Notify Participants within a Perspective Hierarchy
Perspective Management	Perspective Hierarchy Maintenance	Create Issue for Perspective Hierarchy Definition
Perspective Management	Perspective Hierarchy Maintenance	Review Perspective Hierarchy Changes
Perspective Management	Perspective Hierarchy Maintenance	Approve Perspective Hierarchy Changes
Perspective Management	Perspective Hierarchy Maintenance	Delete Perspective Hierarchy
Perspective Management	Perspective Hierarchy Maintenance	Create Perspective Hierarchy
Perspective Management	Perspective Hierarchy Maintenance	Edit Perspective Hierarchy
Perspective Management	Perspective Hierarchy Management	View Perspective Hierarchy
Perspective Management	Perspective Hierarchy Management	View Perspective Hierarchy Approval History

Navigator Entry	Activity	Privilege Name
Perspective Management	Perspective Item Maintenance	Create Perspective Item
Perspective Management	Perspective Item Maintenance	Edit Perspective Item
Perspective Management	Perspective Item Maintenance	Create Issue for Perspective Item Definition
Perspective Management	Perspective Item Maintenance	Review Perspective Item Changes
Perspective Management	Perspective Item Maintenance	Approve Perspective item Changes
Perspective Management	Perspective Item Management	View Perspective Item
Perspective Management	Perspective Item Management	View Perspective Item Approval History
Perspective Management	Perspective Item Management	View Perspective Item Assessment Approval History
Perspective Management	Perspective Management	View Perspective Assessment Results
Process Management	Process Assessment	Create Base Object Adhoc Assessment
Process Management	Process Assessment	Create Issue for Base Object Assessment
Process Management	Process Assessment	Complete Base Object Assessment
Process Management	Process Assessment	Review Base Object Assessment
Process Management	Process Assessment	Add Attachments to a Completed Base Object Assessment
Process Management	Process Assessment	Approve Base Object Assessment
Process Management	Process Maintenance	Create Base Object
Process Management	Process Maintenance	Edit Base Object
Process Management	Process Maintenance	Create Action Items
Process Management	Process Maintenance	Complete Action Items
Process Management	Process Maintenance	Create Issue for Base Object Definition
Process Management	Process Maintenance	Review Base Object Changes
Process Management	Process Maintenance	Approve Base Object Changes
Process Management	Process Maintenance	Delete Base Object
Process Management	Process Management	View Base Object
Process Management	Process Management	View Base Object Approval History
Process Management	Process Management	View Base Object Assessment Approval History
Process Management	Process Management	View Base Object Assessment Results
Report Center	Assessment Tools Reports	Run Control Assessment extract
Report Center	Assessment Tools Reports	Run Control Assessment report
Report Center	Assessment Tools Reports	Run Control Assessment Details Report
Report Center	Assessment Tools Reports	Run Assessment Details Report
Report Center	Assessment Tools Reports	Run Compliance Status Report
Report Center	Control Management Reports	Run Control Details Report
Report Center	Control Management Reports	Run Control Scope Report
Report Center	GRC Administration Reports	Change History Report
Report Center	GRC Administration Reports	Pending Activity Report
Report Center	GRC Administration Reports	Worklist Items Requiring Reassignment
Report Center	GRC Security Reports	Run Role Assignment Report
Report Center	GRC Security Reports	Run Unassigned Data Privileges
Report Center	GRC Security Reports	Run Unassigned Security Perspectives - Records
Report Center	GRC Security Reports	Run Unassigned Records Report

Navigator Entry	Activity	Privilege Name
Report Center	GRC Security Reports	Run Record Assignment Report
Report Center	Issues Manage Reports	Run Issue Listing Extract
Report Center	Issues Manage Reports	Run Issue Details Report
Report Center	Process Management Reports	Run Base Object Assessment Extract
Report Center	Process Management Reports	Run Action Items Report
Report Center	Risk Management Reports	Run Risk Control Matrix Extract
Report Center	Risk Management Reports	Run Risk Control Matrix
Risk Management	Consequence Maintenance	Create Consequence
Risk Management	Consequence Maintenance	Edit Consequence
Risk Management	Consequence Maintenance	Review Consequence Changes
Risk Management	Consequence Maintenance	Approve Consequence Changes
Risk Management	Consequence Maintenance	Delete Consequence
Risk Management	Consequence Management	View Consequence
Risk Management	Consequence Management	View Consequence Approval History
Risk Management	Event Maintenance	Create Event
Risk Management	Event Maintenance	Edit Event
Risk Management	Event Maintenance	Review Event Changes
Risk Management	Event Maintenance	Approve Event Changes
Risk Management	Event Maintenance	Delete Event
Risk Management	Event Management	View Event
Risk Management	Event Management	View Event Approval History
Risk Management	Propose Risk	Propose Risk from Risk Management
Risk Management	Propose Risk	Validate Proposed Risk
Risk Management	Propose Risk	View Proposed Risk
Risk Management	Propose Risk	Reject Proposed Risk
Risk Management	Propose Risk	Create New Risk from Proposed Risk
Risk Management	Risk Analysis	Create Risk Analysis
Risk Management	Risk Analysis	Edit Risk Analysis
Risk Management	Risk Analysis	Complete Risk Analysis
Risk Management	Risk Analysis	Create Issue for Risk Analysis
Risk Management	Risk Analysis	Manage Risk Analysis Model
Risk Management	Risk Analysis	View Risk Analysis Model
Risk Management	Risk Analysis	Manage Likelihood Models for Risk
Risk Management	Risk Analysis	View Likelihood Models for Risk
Risk Management	Risk Analysis	Manage Impact Models for Risk
Risk Management	Risk Analysis	View Impact Models for Risk
Risk Management	Risk Assessment	Create Risk Adhoc Assessment
Risk Management	Risk Assessment	Create Issue for Risk Assessment
Risk Management	Risk Assessment	Complete Risk Assessment
Risk Management	Risk Assessment	Review Risk Assessment
Risk Management	Risk Assessment	Add Attachments to a Completed Risk Assessment
Risk Management	Risk Assessment	Approve Risk Assessment
Risk Management	Risk Evaluation	Create Risk Evaluation

Navigator Entry	Activity	Privilege Name
Risk Management	Risk Evaluation	Edit Risk Evaluation
Risk Management	Risk Evaluation	Create Issue for Risk Evaluation
Risk Management	Risk Evaluation	Complete Risk Evaluation
Risk Management	Risk Evaluation	Manage Context Models for Risk
Risk Management	Risk Evaluation	View Context Models for Risk
Risk Management	Risk Evaluation	Manage Significance Models for Risk
Risk Management	Risk Evaluation	View Significance Models for Risk
Risk Management	Risk Evaluation	Delete Risk Evaluation
Risk Management	Risk Maintenance	Create Risk
Risk Management	Risk Maintenance	Edit Risk
Risk Management	Risk Maintenance	Create Risk from Related Components
Risk Management	Risk Maintenance	Create Issue for Risk Definition
Risk Management	Risk Maintenance	Review Risk Changes
Risk Management	Risk Maintenance	Approve Risk Changes
Risk Management	Risk Maintenance	Delete Risk
Risk Management	Risk Maintenance	Create Fin Gov Risk
Risk Management	Risk Management	View Risk
Risk Management	Risk Management	View Risk Approval History
Risk Management	Risk Management	View Risk Assessment Approval History
Risk Management	Risk Management	View Risk Assessment Results
Risk Management	Risk Management	View Fin Gov Risk
Risk Management	Risk Treatment	Edit Treatment Plan for Risk
Risk Management	Risk Treatment	Create Treatment Plan for Risk
Risk Management	Risk Treatment	Create Issue for Risk Treatment
Setup and Administration	Application Administration	Manage Application Configuration
Setup and Administration	Application Administration	Maintain Installation Options
Setup and Administration	Application Administration	Manage Lookup Tables
Setup and Administration	Application Administration	Manage Value Sets
Setup and Administration	Application Administration	Manage Data Synchronization Parameters
Setup and Administration	Application Administration	Manage Content Types
Setup and Administration	Application Administration	Manage URL Repositories
Setup and Administration	Application Administration	Reassign Worklist
Setup and Administration	Application Administration	Manage Assessment Results
Setup and Administration	Jobs and Scheduling	View Job
Setup and Administration	Jobs and Scheduling	Purge Job
Setup and Administration	Jobs and Scheduling	Cancel Job
Setup and Administration	Jobs and Scheduling	View Schedule
Setup and Administration	Jobs and Scheduling	Edit Schedule
Setup and Administration	Jobs and Scheduling	Unschedule Job
Setup and Administration	Module Management	Edit Object Configuration for a Module
Setup and Administration	Module Management	View Object Configuration for a Module
Setup and Administration	Module Management	Create User Defined Attributes
Setup and Administration	Module Management	Edit User Defined Attributes
Setup and Administration	Module Management	View User Defined Attributes

Navigator Entry	Activity	Privilege Name
Setup and Administration	Module Management	Edit Perspectives for a Module
Setup and Administration	Module Management	View Perspectives for a Module
Setup and Administration	Module Management	Create Module
Setup and Administration	Module Management	Edit Module
Setup and Administration	Module Management	View Module
Setup and Administration	Module Management	Create Import Template
Setup and Administration	Module Management	Import Data File
Setup and Administration	Security Administration	Create Data Role
Setup and Administration	Security Administration	Edit Data Role
Setup and Administration	Security Administration	View Data Role
Setup and Administration	Security Administration	Create Duty Role
Setup and Administration	Security Administration	Edit Duty Role
Setup and Administration	Security Administration	View Duty Role
Setup and Administration	Security Administration	Create Job Role
Setup and Administration	Security Administration	Edit Job Role
Setup and Administration	Security Administration	View Job Role
Setup and Administration	Security Administration	Create User
Setup and Administration	Security Administration	Edit User
Setup and Administration	Security Administration	View User
Setup and Administration	Security Administration	Import Users from LDAP
Welcome	Analytics	View Open Issues by Business Entity graph
Welcome	Analytics	View Open Issues by Severity graph
Welcome	Analytics	View Over Due Remediation Plans graph
Welcome	Analytics	View Issue Overview graph
Welcome	Analytics	View Remediation Plans by Percent Complete
Welcome	Analytics	View Control Assessment Status Overview graph
Welcome	Analytics	View Control Trend by Cost graph
Welcome	Analytics	View Control Trend by Count graph
Welcome	Analytics	View Compliance Status Overview graph
Welcome	Analytics	View Assessment Status Overview graph
Welcome	Analytics	View Issue Counts by Status and Likelihood graph
Welcome	Analytics	View Risk Overview by Context graph
Welcome	Analytics	View Risk Significance by Context graph
Welcome	Analytics	View Base Object Action Item Status graph
Welcome	Analytics	View Base Object Issue Status graph
Welcome	Analytics	View Base Object Overdue Assessment Status graph
Welcome	Analytics	View Quick View
Welcome	Analytics	View Risk Count by Context graph
Welcome	Analytics	View Risk Count by Significance graph
Welcome	Analytics	View Risk Count By Type graph

Navigator Entry	Activity	Privilege Name
Welcome	Analytics	View Control Count By Type graph
Welcome	Intelligence	GRC Home Page Intelligence Tab
GRC Intelligence	Launch GRCI Application	GRC Intelligence Menu Link
Risk Management	Intelligence	Risk Intelligence Tab
Control Management	Intelligence	Control Intelligence Tab
Base Object Management	Intelligence	Base Object Intelligence Tab
Issue Management	Intelligence	Issue Intelligence Tab
Assessment Management	Intelligence	Assessment Intelligence Tab
Welcome	Welcome Dashboard	GRC Application Log in
Welcome	Welcome Dashboard	Manage User Preferences
Welcome	Welcome Dashboard	Propose Risk from GRC Dashboard
Welcome	Welcome Dashboard	Complete Survey
Welcome	Welcome Dashboard	Complete Assessment from GRC Dashboard
Welcome	Welcome page	GRC Application Log In

Disable the Financial Governance Module

EGRCM is delivered with the Financial Governance module. If you are not using this module and do not want it to be displayed within the Navigator, do the following:

1. Do not include the seeded job role Financial Governance Module in any of your users' profiles.
2. Do not include the privilege Display Financial Governance in the Navigator in any of your custom duty roles.

You should not disable the Financial Governance module until you have successfully completed the implementation and configuration of your custom module, because you may need to review functional behavior within Financial Governance as a basis for your custom module.