# Oracle® Enterprise Governance, Risk and Compliance Manager

Implementation Guide

Release 8.6.4.5000

**Part No. E38968-02**

March 2013

Oracle Enterprise Governance, Risk and Compliance Manager Implementation Guide

Part No. E38968-02



Primary Author: David Christie

# Contents

# 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 Manager 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 Certifications Document* 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 *Certifications Document* for recommended and supported hardware configurations.
3. Look on My Oracle Support for known environment variable issues.
4. Follow instructions in the *Oracle Enterprise 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 "Security Management" chapter in the *Oracle Enterprise Governance, Risk and Compliance 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.

## 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 other GRC documentation, in which you can find full information about the procedures for completing each step.

As you set up EGRCM, you must also configure its security — define job roles and their constituent duty roles and data roles, define users, and assign job roles to users. To do so, complete a distinct security checklist, which is available (along with a detailed discussion of security implementation) in the *Oracle Enterprise Governance, Risk and Compliance Security Implementation Guide*.

### 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 created a user based on the admin user (see step 5 of “Diagnostic Steps” on page 1-3). 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 *GRC Installation Guide*.

☐ **3** **Optional:** EGRCM can connect, and supply information, to Oracle Fusion GRC 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.

See the *GRC Installation Guide*.

☐ 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 Certifications Document* 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 the *GRC Installation Guide*.

☐ 5 **Required:** Specify the currency used by your installation of EGRCM. (Only one currency is supported throughout the installation.) Set this value before any data is loaded the application. In the Currency list box of an Installation Options page, select the currency you want to use. (See "Managing Installation Options" in the *GRC User Guide*.)

You can change this value after data has been imported. However, this will not change existing data; it will only change the default itself.

## 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?

See "Module Object Configuration" (page 1-8) as well as "Configuring Module Objects" in the *GRC 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 add a

value for Issue Severity. Not all delivered lookup-table attributes can be modified — see “Managing Lookup Tables” in the *GRC 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 19 in this checklist, “ Creating User Defined Attributes” on page 4-5, and “Managing User-Defined Attributes” in the *GRC User Guide*.

☐ **9** **Required:** Prior to defining perspective hierarchies, think how data-level security applies to the user community. Perspectives are used to define sets of data to which users have access. Perspective hierarchies provide structure to the objects being managed in the application, by grouping objects together in 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. When defining 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 *GRC Security Implementation Guide*.

☐ **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 covers objects like processes, risks, controls, perspectives, and so on, and their relationships. Refer to steps 22 and 23 in this checklist.

## Module Management

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

- ☐ **11** **Required:** To define a new module, a user must select a template, called the Standard template. It 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 *GRC User Guide*.

- ☐ **12** **Required:** Select objects for the module. Prior to configuring a new module, 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, include that object as part of the new module. The object can easily be enabled at the appropriate time. Review the module definition carefully — once submitted, it 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. 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.

- ☐ **13** **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.

- ☐ **14** **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

☐ **15** **Required:** Base object, risk, and control have configuration options, and each object has characteristics to support its business objective. For example, the risk object is designed to support risk-management elements, while the control object is designed to support test plans and instructions. 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 16–18.

☐ **16** **Optional:** 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 later these features may be required. In the Financial Governance module, events and consequences are hidden; treatments are set to "Hide and Default," meaning that treatments and treatment plans are hidden, but related control stratification is exposed. In custom modules, all these features default to "Show." Even if events, consequences, or treatments are not needed immediately, consider turning (or leaving) these features on and leveraging job roles to restrict access to them.

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

☐ **17** **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).

☐ **18** **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 17) also apply to control-object configuration.

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

## User-Defined Attributes for Objects within a Module

- ☐ **19** **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 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

- ☐ **20** **Required:** Review how perspectives are to be managed. If you use new perspective types, you must define these prior to defining the perspective.
- ☐ **21** **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. Also, EGRCM supports granular data-level security through perspective values assigned to data roles. 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. 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 *GRC Security Implementation Guide*.

## Operational Data Definition

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

- ☐ **22** **Required:** Operational data can be loaded into the application for Financial Governance and new module objects, through use of an import template Excel spreadsheet. Refer to Chapter 5, "Importing Operational Data."
- ☐ **23** **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," in the *GRC Security Implementation Guide*.

## Assessment Management Definition

- ☐ **24** **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 "Survey Management" in the *EGRCM User Guide*.

- ☐ **25** **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 "Managing Assessments" (page 6-1) of this document as well as "Assessment Management" 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 User Guide* for help in completing setups.

## Managing 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 “Application Configuration Management” in the *GRC User Guide*.

## Installation Options

Consider what you want the currency to default to as you build out the application data. This option is generally set during implementation, but can be changed at any time. Remember that changing this value impacts the entire installation. However, changing the default currency will not change the values that already exist within the application data. Any change takes 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 *GRC User Guide*.

3

# Financial Governance Configuration

EGRCM Financial Governance is a seeded module; users 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. Users can hide or display specific features, such as events that are available within the risk object. Users 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:

- A Process object is the parent of a Risk object, which is the parent of a Control object.
- A Perspective object is available to each of the Process, Risk, and Control objects, and each of these objects can generate Issues.

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 requirements may 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, 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).

## Configuring 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.

## Managing Seeded Content

The Financial Governance module includes the following seeded content:

- Risk models: Analysis, Likelihood, Impact, Significance, and Context
- 302 SOX Certification Questions within Survey Management

This data has been provided to aid setting up new risk models and new certification questions. It is recommended that the seeded data not be used directly. Make copies and, if needed, make changes to the copies. Then reference this new data. This is recommended for two reasons, to ensure upgrade persistence and to support data migration. Making copies ensures that changes made to models and questions are maintained after a patch or new release is applied. Additionally, seeded data is not exported when the Data Migration utility is used, so it is not possible to import new risk data that references the seeded models. It is also not possible to export risk data added through the UI that references the seeded data and update that via the import template to be reloaded. The import of that data will receive an Invalid Reference error, because the seeded models are not exported and not contained within the import file.

## Managing Perspectives

The Financial Governance module does not include seeded perspectives. Define and configure the perspectives you need to provide context to the Financial Governance objects. You can define perspectives through the UI or use the Data Migration utility to import them with your operational data. Refer to Chapter 5, "Importing Operational Data," for guidance on using this utility.

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 Recovery 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.

## Configuring and Managing 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.

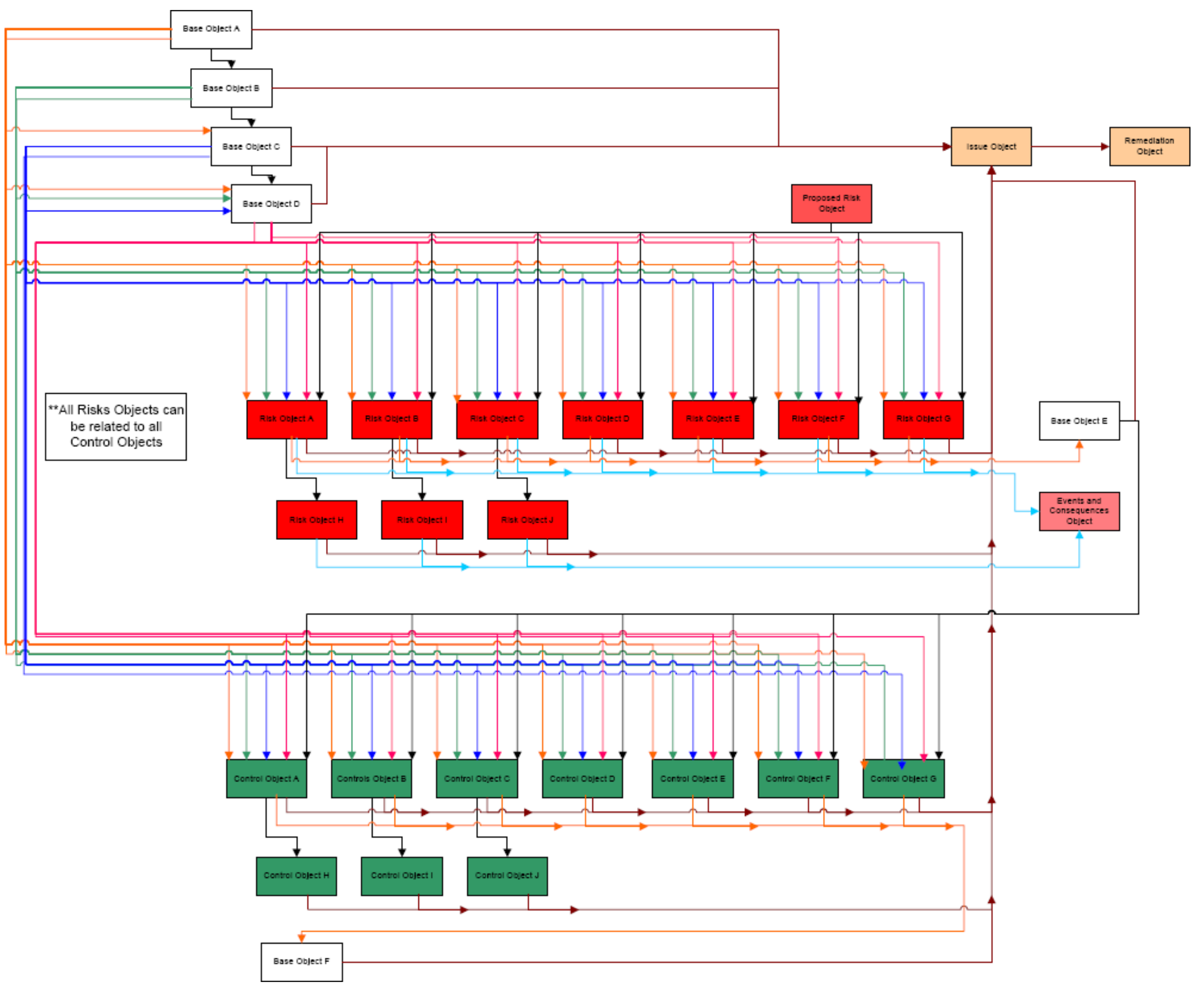
## Creating a New Module

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 *GRC 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 *GRC Security Implementation Guide*).

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 *GRC 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 “Other Setup Options” chapter in the *GRC 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 operational data for the Financial Governance module or any new module defined through use of the Data Migration utility. This consists of generating an XML template that reflects the specific configurations defined for the module, updating this file with your operational data for the module, and running the import process.

The import template supports uploading the following:

- Perspective data
  - Perspective item
  - Perspective
  - Perspective hierarchy
- Object data
  - Process
  - Risk, including subordinate event, consequence, treatment plan, treatment
  - Control, including subordinate test plan, test instruction, and test step
  - Base object (as part of a new module)
  - Risk models, including likelihood, impact, analysis, significance, and context models
- Association data
  - Associations between risk and control, identifying which risks are associated with which controls
  - Associations between process and risk, identifying which processes are associated with which risks
  - Associations between perspective and other objects, identifying which perspective values are associated with which objects
  - Associations available within the standard template for a new module. These include base object and another base object; base object and risk; base object and control; risk to another risk object; risk to base object; control to another control object; control to base object.

- Transaction data
  - Issues for control, process, base object, perspective, and assessments
  - Remediation plans for issues
  - Action items for process and base objects
  - Risk analysis
  - Risk evaluation
  - Assessments for risk, control, process, base object, and perspective
- Attachments
  - For object data — process, risk, control, and base object
  - For transaction data — issue, remediation plan, action item, risk analysis, risk evaluation, and assessment
- Loading a library from a provider: Map the library data to the import template. Library data can be incorporated with the initial import or imported later.

Data Migration supports two methods of importing data:

- Initial Load: The import file contains operational data that is new to the module and has no association to data already existing in the module. (Initial Load can be run even when other data already exists in the module.)
- Incremental Load: The import file once again contains operational data that is new to the module, but it may define associations to data that already exists in the module, or new values for perspectives that already exist in the module. New transaction data for existing objects can also be imported during an incremental load, but the update of existing transactions is not supported.

Regardless of import method, the import template must be generated for a module through use of the Data Migration page within the application. The configuration metadata about the module is used to produce the import template, and only the objects configured for the module are included in the template. All user-defined attributes defined for each object will be included in the data structure for that object in the template.

## Prerequisites

Before importing data, ensure that the following tasks are completed:

- All points within the Administration Setup section of this document are complete. 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 (including the object type codes). If new UDAs are added after the import template is generated, you will need to generate the import template again.

  For additional information, refer to Chapter 2, “Administration Setup.”
- Perspective type codes are defined. Before the import script is run, the perspective type used for the perspective must be defined. The template supports creating new perspectives with corresponding values within the

template worksheet. Associations of perspective items to the perspective hierarchy are by the perspective type code. The perspective type code provides the means to tie the perspective hierarchy to values.

- The perspective type code should be in capital letters with no spaces.
- The application is delivered with several perspective type codes. Create new codes by using the Manage Lookup Table page within Setup and Administration. The lookup type is GRCM_PERSPECTIVE_TYPE, and available codes are entered in the Lookup Code field. Add new perspective type codes as new lookup codes for GRCM_PERSPECTIVE_TYPE.

For more information, see “Managing Lookup Tables” in the *GRC User Guide*.

- Review the setup and configuration of the module to verify it is complete. Many settings *cannot be changed* once data is imported. The environment must be set up with all the system data installed and configurations set *before data is imported*. For example, ensure that the module definition is complete, with all appropriate objects and object associations defined, Hide/Show/Default Treatment for the risk object is configured, module object perspective associations are properly defined, and so on.
  - If you are importing data for the Financial Governance module, see Chapter 3, “Financial Governance Configuration,” for additional information.
  - If you are importing data for a new module, refer to Chapter 4, “Module Management,” for additional information.
- Take a backup of the database just prior to running the import process and after all the setup and configuration is complete. This provides the ability to restore the instance and back out the imported data if the data load is not to your satisfaction.

## Generating the Import Template

Use the Data Migration page in Setup and Administration to generate the import template for a module.

1. Log into the application. Select Setup and Administration in the Navigator, and then select Data Migration in the Module Management list of tasks.
2. Select the module name in the Available Modules grid, and then select the Create Import Template action.
3. Indicate whether the template is to contain existing operational data for the module.
   - When generating a template for the initial load of operational data, do not include the existing module data. Select Without Data.
   - When generating the import template for an incremental load, indicate to include module data. The existing module data must be included in the import template to support defining new associations to it.

     Select With Data — All Objects to create an import template that includes all the existing perspective, object, and association data.

Select With Data — Perspectives Only to create an import template with just the perspective data in it. The file will contain only the three perspective data worksheets.

- Exporting the existing module data into the import template has the following restrictions:

  The process respects the current user's data access. Only the objects to which that user has access are exported. Therefore if all data should be exported, a user with access to all the data (i.e., a super user) should create the import template to ensure that all module data is exported. Refer to step 23 in the Setup Checklist (see page 1-9).

  All user-defined object data, association data, and perspective data (both active and inactive) is exported. Transaction data and attachment data cannot be exported.

  When data is exported for a module, all perspectives are exported. Perspectives are not module-specific, and may be referenced by any GRC module.

  Seeded data is not exported. The impact of this is that data within the import template cannot refer to the seeded data. For example, the Financial Governance module is delivered with risk models defined to support risk analysis and evaluation activities. It is not possible to import new risks and have them use these seeded models, since they will not be included within the import template. Refer to "Managing Seeded Content" on page 3-2.

4. A message presents a job number. Note the number, then close the message (click on its OK button).
5. Navigate to the GRC Manage Jobs page. (Select Manage Jobs among the Setup tasks in the Navigator.)
6. In the Manage Jobs page, locate the row displaying the job ID you noted in step 4. In its Message cell, click on the Job Completed link.
7. A Job Detail window opens. In it, click on the Job Results link.
8. A File Download window offers you options to open or save the export file. Click on its Save button and, in a Save As dialog, navigate to a folder in which you want to save the file.
9. Close the Job Detail window (click on its OK button).

It is good practice to make a copy of the XML file as a backup before adding or changing the data within it. This is most important if the import template is created with the existing application data. The backup file can be referenced to reset data that may accidentally get changed while the file is populated.

## Understanding the Import Template

The system generates an XML file that contains all the objects and their data structure for the selected module, and writes the file to the specified location. The XML file is designed to support using Excel to view and update it. It is organized so that each object, each association, and each transaction is viewed in its own worksheet.

For example, the PerspectiveItem worksheet includes perspective values, and the Risk worksheet contains risks to be loaded in the database for the module. The PerspectiveItemRisk worksheet identifies the association between risk and perspective.

The first row of a worksheet identifies the name of the object. The second row identifies data columns for this object; in addition to column name, it identifies the column type (String, Integer and so forth) and whether the field is required in the database.

- Do not remove these rows or change any data in them.
- If the import template was generated with module data, the existing data appears within each of the worksheets following row 2.

There are two ID columns within the object worksheets. The first ID is the worksheet ID and is used to relate the data within the spreadsheet. The second ID is the encrypted system ID and is populated only for existing data. It is used by the import process to identify the existing data.

If the template was generated with module data, the worksheet ID and the system ID are assigned to the row. Do not change these. All the exported associations reference the worksheet ID, and if it is changed the worksheet ID will be out of sync between the object worksheet and the association worksheets.

Each object worksheet (Perspective, Risk, Control, Process, Base Object) has a STATE_CODE(String)(Required) column. This is the state for the record once it is loaded. Depending on the object, you can import data in either NEW, REVIEW, or APPROVED state.

- If the data is imported in NEW state, manual user intervention is needed before it can be used within the module. Like new data that is entered through the UI and "Saved," the user will have the extra step of opening the data within the UI and then submitting the data. Be advised that no worklist is generated for records loaded in the NEW state.
- If the data is imported in REVIEW state, the review and approval workflow gets initiated for it once it is loaded. Each record imported in the state of REVIEW generates worklist entries for the appropriate users. Data will stay in the REVIEW state until the review and approval workflow is completed for it and before it is considered active data for the module. Consider using this state once the module is in production and the import is updating existing data as an extra precaution for changing production data.

  Since the normal review and approval workflow is initiated, when the system finds no user assigned to complete the review, the review step is skipped and the workflow moves to the approval step. Likewise if no user is found to complete the approval the state will be set to APPROVED as if the review and approval process had been completed by a user.
- If the data is imported in APPROVED state, the data is immediately available for use by the module after import. For the initial load of data, it is recommended that data be imported in the APPROVED state.

Each object worksheet (Perspective, Risk, Control, Process, and Base Object) has a REVISION_NUMBER (Integer) column. This column is populated for the existing module data and is the current revision number for the record when it was exported. Do not set this for new data. For additional information on the REVISION_NUMBER, refer to "Using the Import Template for an Incremental Load" (page 5-12).

## Populating the Import Template

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

- The first column of each worksheet contains worksheet ID values, and each must be unique within its worksheet. When existing module data is contained with the worksheet, the worksheet IDs are already assigned.
- The worksheet ID is not saved in the database, but plays an important role in identifying associations between objects on the spreadsheet. Therefore you can use whatever numbering system helps you best organize your data. This system must, however, use numeric values. Keep it as simple as possible. When data exists in the template, it is recommended that you start the new worksheet IDs with a number greater than the last ID assigned to the existing data, so that it is easier to identify the new data. Keep in mind that for each type of object (base, risk, and control), the worksheet ID must be unique across the set of objects.
- For new object data, the second system ID must be blank.
- Populate each object worksheet with operational data appropriate to the object identified in row one of the worksheet. Use the UI pages to assist you in understanding the columns listed in each worksheet. Each column in an object worksheet generally corresponds to a field visible within the create and edit page for that object.
- When left blank, STATE_CODE is set to APPROVED. Complete this field only when you want a state other than APPROVED.
- If existing module data is contained within the worksheet, add the new rows to the worksheet following the existing data. If you want to add a "tag line" in the worksheet to denote the start of the new data, this must be removed before the import is run. It is not recommended that you intersperse new data within the existing data. If a new record is to be similar to an existing record, copy the existing record, paste the copy to the end, and edit it there. Be sure to remove the system ID from the new row created when you copy an existing data row.
- Be careful not to add a value for the NAME column that exceeds 150 bytes.
- Do not include carriage returns within any of the text fields, such as the object name and description fields. Carriage returns used for formatting text within a cell signify the end of the text when validations such as duplicate name are performed, and can result in errors.
- Do not use the following special characters in text fields: & ' # < > * =. These characters have special meaning in Excel and XML.
- Add values that match the data type of the column. If the data type is listed as Integer or Double, do not enter character text.
- When the worksheet contains the ACTIVITY_CODE column, as on the TestPlan worksheet or the Assessment worksheet, use a code from the following table. Enter codes exactly as listed. Not all activity codes are appropriate for the various objects. Refer to the "Assessment Management" chapter of the *EGRCM User Guide* for information on which assessment activities are used by the various objects.

| Activity Code | Activity Description |
|---|---|
| ASSESS_RISK | Risk assessment |
| AUDIT | Audit |
| AUDIT_TEST | Audit test |
| DESIGN_ASSESS | Design assessment |
| DOC_UPDATE | Documentation update |
| CERTIFY | Certification |
| OPERATING_ASSESS | Operating assessment |

- If the field is controlled by a lookup table, only use valid codes. Go to the UI page where this data is entered. If field values are presented as a list of values, you need to add the appropriate code. To find the set of codes for each lookup table, use the Manage Lookup Tables page within Setup and Administration and search by Meaning.
- If the field is a checkbox within the UI, enter Y to indicate that it is selected or N to indicate it is not selected.
- During template generation, UDA columns were added to the import template based on the configuration. Complete them with the appropriate values.
- Each object worksheet (Perspective, Risk, Control, Process, and Base Object) has a REVISION_NUMBER (Integer) column. This column is populated for the existing module data and is the current revision number for the record when it was exported. Do no populate this column for new data.
- 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 a Control” in the *EGRCM User Guide*.)
- The worksheet to complete for the Risk relationships to Control depends on the configuration option selected for Treatment on the Risk object.
  - Show: Complete the TreatmentPlan, Treatment, and TreatmentControl worksheets.
  - Hide and Default: Complete the RiskControl worksheet.
  - Hide: Complete the ObjectRelation worksheet. This is appropriate only for a new module and only if the Risk object in that module is related to a Control object.

## Perspective, PerspectiveItem, and PerspectiveHierarchy Worksheets

Use three worksheets to create perspective hierarchies:

- The Perspective worksheet establishes the perspectives themselves. Among other values, each row contains the name of a perspective hierarchy and the perspective type code that applies to it.
- The PerspectiveItem worksheet defines perspective values. Each row names a value and relates it to the perspective type code configured for a hierarchy (in

the Perspective worksheet). The worksheet contains values for any number of hierarchies.

- The PerspectiveHierarchy worksheet determines the hierarchy structure of each perspective. Each row defines a parent/child relationship between two values created in the PerspectiveItem worksheet, and relates the pair to a hierarchy defined in the Perspective worksheet.

In the Perspective worksheet:

- Each row contains information which, once the file is imported, can be found in the Definition section of the Perspective Management page (under Tools in the GRC Navigator).
- The perspective type code (PERSP_TYPE_CODE) for a given hierarchy must be the same as the code for the values it contains (as defined in the PerspectiveItem worksheet).

In the PerspectiveItem worksheet:

- The record for a perspective value does not define its relationship to a perspective hierarchy.
- Even so, the PERSP_TYPE_CODE indicates a perspective hierarchy type. The code for each value (each PerspectiveItem row) must match the code created in the Perspective worksheet for the hierarchy to which that value belongs.
- Each perspective value can exist in only one perspective hierarchy.
- PerspectiveItem name cannot exceed 50 characters.

In each row of the PerspectiveHierarchy worksheet:

- Populate the PERSP_ITEM_NAME cell with the name of a value (defined in the PerspectiveItem worksheet) that is the parent of another value.
- Populate the CHILD_NAME cell with the name of a value (defined in the Perspective Item worksheet) that is the child of the value in the PERSP_ITEM_NAME cell.
- Populate the TREE_NAME cell with the name of the perspective hierarchy (defined in the Perspective worksheet) to which both values belong.
- Enter the letter Y in the ROOT cell if the PERSP_ITEM_NAME cell contains the root (top-level) value of the perspective hierarchy. Enter the letter N if it does not.

## Association Worksheets

Populate the Association worksheets for object associations. This involves identifying associations between objects — for example risks that have associated controls. It also involves identifying associations between objects and perspectives — for example, controls that belong to a given organization.

Each Association worksheet includes worksheet IDs established in the worksheets that define objects or perspective items. Each row in an Association worksheet pairs two of these IDs, thus establishing an association between the entities they represent — two objects, or an object and a perspective value.

For example, the following table presents values that might be entered in the PerspectiveItemControl worksheet:

| PERSP_ITEM_ID | CONTROL_ID |
|---|---|
| 1 | 1 |
| 2 | 2 |
| 3 | 3 |
| 4 | 1 |
| 4 | 2 |
| 4 | 3 |

The worksheet IDs entered in this worksheet match worksheet IDs from the Control and PerspectiveItem worksheets. For example, the control whose worksheet ID is 1 in the Control worksheet is associated with two perspective values — those with worksheet IDs 1 and 4 in the PerspectiveItem worksheet.

Also, controls 1, 2, and 3 share a perspective value because, in the bottom three rows of this example, each is associated with worksheet ID 4 from the PerspectiveItem worksheet.

### *Populate the Associations for Objects in the Standard Template for A New Module*

As you populate an import template for a new module based on the standard template, consider these points:

- Enter all Perspective to Flex-Base-Object relationships in the PerspectiveItemProcess tab. The worksheet ID for all the types of process or base object must be unique across the set of base objects. This worksheet is used because Process is a base object.
- Enter all the Perspective to Flex-Risk-Object relationships on the PerspectiveItemRisk tab. The worksheet 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 worksheet 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 listed on line one of their worksheets such as FLEX_OBJECT_CONTROL_A.
- The ID is the worksheet ID for the object on the worksheet as used in any other relationship definition. The worksheet ID for all types of risk and control objects must be unique across the set of objects.

## Attachment Worksheet

Specify attachments in the Attachment worksheet.

There are two attachment types: Desktop File and URL. For you to import a desktop-file attachment, the file must exist on the EGRCM server. Copy it there if it is not located there already.

Populate the Attachment worksheet with an ID, Name, and Description similar to those of other objects. Populate other columns as follows:

| Column | Value |
|---|---|
| ATTACHMENT_TYPE | Enter a code appropriate to the attachment: DESKTOP_FILE or URL. (These codes are defined in the GRC_ATTACHMENT_TYPE table). |
| FILE_NAME | If you selected DESKTOP_FILE as the attachment type, enter the fully qualified path and file name for the file residing on the server. If you selected URL as the attachment type, leave this column blank. |
| CONTENT_TYPE | If you selected DESKTOP_FILE as the attachment type, enter the appropriate content type code for this attachment. (Content types are defined within Manage Content Types in Setup and Administration.) Content type does not apply to the URL attachment type. |
| URL | If you selected URL as the attachment type, enter the actual URL for the attachment. If you selected DESKTOP_FILE as the attachment type, leave this column blank. |
| OBJECT_TYPE_CODE | The object type code for the object the attachment is for. Object type code is the name of the object listed on line 1 of its worksheet. |
| OBJECT_ID | The worksheet ID for the record the attachment is for. |

## Transaction Worksheets

To upload issues:

- Complete the Issue, RemediationPlan, RemediationTask worksheets. Enter the relationships for the issues on the IssueRisk, IssueControl, IssueProcess, IssuePerspective, and IssueRemediationPlan worksheets.
- If you are loading issues for one of the base object record types within the standard template, use the IssueProcess worksheet.

To upload risk analysis:

- Populate the following risk model worksheets as needed — RiskAnalysisModel, RiskAnalysisImpactModel, RiskAnalysisLikelihoodModel, RiskAnalysisRisk LevelMapping, LikelihoodModel, LikelihoodParameter, ImpactModel and ImpactParameter. EGRCM supports “qualitative” and “semi-quantitative” risk analysis. Refer to the UI pages to define the models for the columns that need to be populated for each type. The following table contains codes that appear on risk analysis model worksheets. Choose an appropriate code from this table.

| Column Name | Code | Description |
|---|---|---|
| ANALYSIS_TYPE_CODE | QUAL | Qualitative |
| | SQUAN | Semi-quantitative |
| LIKELIHOOD_TYPE | QUAL | Qualitative |
| | SQUAN | Semi-Quantitative |
| TIMEFRAME_CODE | DAY | Per day |
| | WEEK | Per week |
| | QUARTER | Per quarter |
| | YEAR | Per year |
| | DECADE | Per decade |
| | CENTURY | Per century |

- Populate the RiskAnalysis worksheet with analysis results.

To upload risk evaluation:

- Populate the following risk model worksheets as needed – ContextModel, ContextModelRiskCriteria, ContextModelRiskCriteriaDetail, SignificanceModel and SignificanceModelDetails. These worksheets contain several codes that must be populated appropriately.
- Populate RiskEvaluation worksheet with the evaluation results. The following table lists the available values for TOLERANCE_CODE.

| TOLERANCE_CODE | Description |
|---|---|
| 1 | Accepted |
| 2 | Monitor |
| 3 | Treat |

To upload assessments:

- Populate the Assessment worksheet for the assessment definition.

  OBJECT_TYPE_CODE identifies the object the assessment is for. Populate this column with the appropriate code from this table.

| Object Type Code | Description |
|---|---|
| GRC_CONTROL | Control |
| GRC_RISK | Risk |
| GRC_PROCESS | Process or Base Object |
| GRC_PERSP_ITEM | Perspective |

  Note: Even if the assessment is for an object within the standard template, use the corresponding object type from the table above. For example, if the assessment is for controls that belong to FLEX_OBJECT_CONTROL_A in a new module, use GRC_CONTROL as the object type for the assessment.

- Populate the specific object Assessment worksheets for the assessment results. Each object has a separate worksheet — RiskAssessment, ControlAssessment, ProcessAssessment, PerspectiveAssessment.

  Note: For assessment responses against base objects in the standard template, use the ProcessAssessment worksheet to enter assessment responses.

When importing assessment results for the additional types available within the standard template, use this same set of object assessment worksheets.

Set the RESPONSE_CODE to represent overall assessment results. The meaning of each code is maintained in the Manage Assessment Results page (in Setup and Administration). Refer to this page for the configured meaning associated to each code. Complete each Assessment worksheet with the appropriate one of the following response codes:

– NO_OPINION
– AGREE
– AGREE_WITH_EXCEPTION
– DO_NOT_AGREE
– OUT_OF_TOLERANCE
– REQ_EVALUATION
– REQ_ADDITIONAL_ANALYSIS
– REQ_DOCUMENTATION
– MEETS_GUIDANCE
– PASS
– PASS_WITH_EXCEPTION
– FAIL
– COMPLETED
– NO_ACTION
– NOT_STARTED

## Using the Import Template for an Incremental Load

To support an incremental load, use one of the With Data options as you generate the import template, so that existing data is included. These options include With Data — All Objects and With Data — Perspective Only.

- When a With Data option is used, all the appropriate module data is included within template in its corresponding worksheet. For each record, the worksheet ID is populated and the system ID contains encrypted system information. Transaction and attachment data is not included. The encrypted system ID is used to determine that the record already exists within the application.
- Exported data respects the security of the user creating the import template. Only the data to which that user has access is exported. Therefore if all data should be exported, a user with access to all the data (i.e., a super user) should create the import template to ensure that all module data is exported. Refer to step 23 in the Setup Checklist (see page 1-9).
- Existing data is exported so that new data can be associated to it. The import process cannot update existing data. File data with a value in the system ID column

is not processed during an import, except to define a new association between new and existing data in the file.

- When existing data is associated to new data, the import process generates a new version of the existing object. Its state is set to Review, and the new version enters the review/approval workflow as if it were updated through the UI.
- To add a new perspective item to an existing perspective:
  - Add the new value to the PerspectiveItem worksheet and assign it a unique worksheet ID.
  - Add the new value in the Perspective Hierarchy worksheet to define where it is to be inserted into the existing hierarchy.
  - When a new perspective item is added to the perspective hierarchy, the import process generates a new version of the perspective. The state is set to Review, and the new version enters the review/approval workflow as if it were updated through the UI.

## Using Data Migration to Move Data to Another Instance

You can also use the Data Migration utility to move data from one instance to another — for example, from a development environment to a test environment.

1. Create the import template for the module data you want to move from the source environment, for example the development environment. Select one of the With Data options depending on whether you are moving all the operational data or just perspective data.

   Exported data respects the security of the user creating the import template. Only the data to which that user has access is exported. Therefore if the intention is to migrate all the data, the user who creates the import template must have access to all the operational data.

2. Use Excel to review the import file you have created.
   - Since all data was exported, remove data you do not wish to migrate. For example, if you used the With Data — Perspectives Only option as you created the import file, the file includes all perspectives defined for the selected module. However, you may not want or need to move all perspectives. In this case, remove unwanted perspectives from the import file. For each:
     - Remove the perspective from the Perspective worksheet.
     - Remove the parent/child relationships from the PerpsectiveHierarchy worksheet.
     - Remove all the perspective values for this hierarchy from the PerspectiveItem worksheet.

     Be sure to make a backup copy of the file before you start to remove data.

     Note: Removing data from the import file may require you to remove data from multiple worksheets as in the PerspectiveItem, Perspective, PerspectiveHierarchy, and the Perspective object associations worksheets (i.e., PerspectiveItemControl associations). When data is removed, all references to that data from all the worksheets must be removed or you will receive “Invalid Object Reference” errors.

- Review the data for codes referenced by objects included in the import file, and for UDAs. You must ensure these are defined in the target environment before you load data to that environment.

  For example, the PerspectiveItem worksheet contains perspective type codes. If any are missing from the target environment, use Manage Lookup Tables in Setup and Administration to add them to the GRCM_PERSPECTIVE_TYPE lookup table.

- The new data is loaded by default at the Approved state. If this is not the state you desire, set the STATE_CODE within the import file.

**3.** Use the Initial Load option to load the data into the target environment.

Never use the Incremental Load option when migrating data. With this option, the encrypted system data is used to update existing records. This will result in corrupt data in the source environment.

## Import Checklist

Before running the import, complete the following import checklist:

- ☐ Administration setup is complete.
- ☐ Module configuration is complete.
- ☐ Lookup tables have been updated with new codes.
- ☐ Make sure that the import template is not saved with empty cells highlighted. Otherwise the import will generate Null error messages. Tip: Go through each worksheet and put your cursor in cell A1.
- ☐ Make sure there are no duplicates in the Name and Worksheet ID columns in all the worksheets. Otherwise the import will generate duplicate error messages. See “Finding Duplicate Names” (page A-2).
- ☐ Remove any formatting, tags, rows, or formulas you may have added to the worksheet to help you complete it.
- ☐ Remove all data filters, if any, from each worksheet sheet.
- ☐ Remove all carriage returns within text fields and ensure that special characters are not used.
- ☐ Be sure the template is saved as XML Spreadsheet (2003 Excel) or XML Spreadsheet 2003 (*.xml).
- ☐ Ensure that a user is defined to have access to view all the data being imported.
- ☐ Optional: Back up the database.

## Running the Import Process

The import process has the following constraints:

- Initial Load supports importing new data that has no relationship to data already existing in the module. You can use the initial load method multiple times, as long as all data in the template is new and unrelated to data existing in the module.
- Incremental Load supports importing new data that has relationships to existing data.
- An import can apply the Initial Load option to an XML file generated with existing module data, for example to load a file from one instance to another. In this case, the system loads all the data as new data and does not attempt to determine if records exist or not.

  If you use an XML file generated from one instance to load into another instance, you must use the Initial Load option. Refer to "Using Data Migration to Move Data to Another Instance" (page 5-13).

  Be aware that the target instance must have the same module configuration, same configured UDAs, and all the lookup codes defined before the import is run. Refer to "Import Checklist" (page 5-13).
- The import utility supports loading data in the New, Review, or Approved state.

  If data is imported with the New state code, import records will exist immediately with the status/state of Active/New. These records will have to be approved within the application.

  If data is imported with the Review state code:

  – Imported records will exist immediately with the status of Active. State will be determined by the Review and Approval workflow.

  – The system will initiate the Review and Approval workflow for this record.

  – If a user is found who can complete the review for a given record, its State is set to Review, and a worklist is generated for the appropriate user.

  – If no user is found for the review step, the record progresses to the approval step. If a user is found who can complete the approval for this record, the State is set to Approval, and a worklist is generated for the appropriate user.

  – If no user is found for the approval state, the record state is set to Approved.

  If data is imported with the Approved state code, imported records exist immediately with the status/state of Active/Approved.
- In the imported data, the Created By and Last Updated By values are set to the username of the user who ran the import.

To run the import process:

1. Log into the application. Select Setup and Administration in the Navigator, and then select Data Migration in the Module Management list of tasks.
2. In the Available Modules grid, select the module into which you want to import data. Then click the Import Data File button.

3. In an Import File window, click the Browse button and navigate to the file you want to import. Its path then appears in the field next to the Browse button.
4. In the Import File window, indicate which import method to use:
   - Select Initial Load and the system will load all the data within the file as new operational data for the module.
   - Select Incremental Load when the file contains both new data and updates to existing data for the module.

   Then click the Import button.
5. A message presents a job number. Note the number, then close the message (click on its OK button).
6. Navigate to the GRC Manage Jobs page. (Select Manage Jobs among the Setup tasks in the Navigator.)
7. In the Manage Jobs page, locate the row displaying the job ID you noted in step 5. In its Message cell, click on the Job Completed link.
8. A Job Detail window opens. In it, click on the Job Results link.
9. Review import statistics, including the number of imported records and validation errors, if any. (If validation errors occur, no data is imported. You would need to correct the errors in the import file, then perform the import once again. You can export validation errors to Excel so that correcting the import file is easier.)

## Import Validation

To ensure data integrity, the import process performs validation on the data. The following table lists the types of validation performed and the error message issued when the situation is detected. Refer to “Understanding Import Error Messages” (page A- 1) for a discussion of error-message components.

| 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) |
| All required fields must be completed for a new object<br>Perspective is marked required for the object and is missing | Value is missing for a required attribute (attribute name, sheet name) |
| For new records, the object name cannot already exist within the application. | Object already exists with the name given (attribute name, attribute value, 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) |

| Validation | Error Message |
|---|---|
| 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. |
| The file name specified for an attachment is valid | File name is not found(attribute name, attribute type, sheet name, row number) |
| The object type within the assessment must match the object type it is associated to. | Invalid object type for the assessment being related (attribute name, attribute value, sheet name, row number) |
| The type (Qualitative or Quantitative) must be the same when relating risk model components together. For example, the impact model reference by the analysis model must both be of the same type, either Qualitative or Quantitative. | Type of the related object does not match the type of the object being related (attribute name, attribute value, sheet name, row number) |
| Attachments cannot be imported if GRC is configured to store attachments within UCM. | File Attachments cannot be loaded when storing in UCM (attribute name, attribute value, sheet name, row number) |
| **Incremental Load Specific Validations** | **Error Message** |
| Cannot update an object in a state other than ‘Approved’. | Object state is not appropriate for updating (object name, sheet name, row number) |
| Cannot define an association to an Object unless the status of the associated object is ‘Active’ and the State cannot = New | Referenced object is not in an appropriate state (referenced object name, object name, sheet name, row number |
| The type of an attachment cannot be changed once it has already been loaded. | Attachment type cannot be changed (name, attribute value, sheet name) |

| Validation | Error Message |
| --- | --- |
| **Perspective Specific Validations** | **Error Message** |
| Values entered on the PerspectiveHierarchy worksheet for PERSPERSPECTIVE_ITEM_NAME and CHILD_NAME must be found within the PerspectiveItem tab.<br>Values enter on the PerspectiveHierarchy worksheet for TREE_NAME must be found within the Perspective Tab. | No entity row found for the value given for the entity Id (attribute name, attribute value, sheet name, row number) |
| A CHILD_NAME within the PerspectiveHierarchy worksheet cannot be listed multiple times with different parent values within the same TREE_NAME.<br>Ensure that perspective item values within the CHILD_NAME column is only listed once for a given tree. | Attribute Value given makes the row duplicate(attribute name, attribute value, sheet name, row number, previous row number) |
| The root value within a perspective hierarchy cannot be removed. | Root PerspectiveItem cannot be deleted (perspective tree name, sheet name) |
| Perspective items associated to objects must be within a perspective hierarchy | Perspective Item referenced is not defined in a perspective hierarchy (attribute name, item name, sheet name, row number) |
| Perspective items associated to object must be within a perspective hierarchy that is defined for the module and object type | Perspective Item referenced is not defined in a perspective hierarchy configured for the object type (attribute name, item name, object type, sheet name, row number) |
| Only one perspective item can be marked as the root for a perspective hierarchy. | Perspective cannot have more than one perspective item identified as root (attribute name, attribute value, sheet name, row number) |
| All the child relationships for the root perspective item within the hierarchy must have ROOT set to Y. | Root flag is not set for the root node of the perspective (attribute name, attribute value, sheet name, row number) |

## Leveraging the Incremental Load Feature for Initial Load

The initial load may involve a very large amount of operational data to import for a module. In this case, it would be better to load the data in smaller groups. Leverage the incremental load feature of the import to accomplish this.

1. Determine your strategy for separating this data into groups for importing.

   The Incremental Load option supports only the update of existing data with associations to new data. So you must import the groups of data starting with the highest object in the information model for the module. Then progress downward through the information model of that module. For Financial Governance, that would be Process. Another option might be to import Process and Risk together in the first import.

   For this discussion, assume the following groups for importing data into the Financial Governance module:

   - Perspectives and Process
   - Risk and Control

2. Generate the import template for the Financial Governance module.
    a. Select the Without Data option.
    b. Complete the import template with Perspective, Process, and Perspective Process association data.
    c. Run the first import. Specify Initial Load.
    d. Verify that the data was loaded correctly before proceeding to import the next set of data.
3. Generate the import template for the Financial Governance module again.
    a. Select the With Data option.
    b. Complete the import template with Risk and Control data.
    c. Depending on the configuration options set for the risk object, use either the RiskControl or the TreatmentControl worksheet to define the Risk to Control association. Use the worksheet IDs assigned to the rows in the Risk and Control worksheets to complete the associations.
    d. Complete the Process Risk associations to define which existing Process is related to the newly added Risk. Use the worksheet IDs assigned to the rows with the Process and Risk worksheets to complete the associations.
    e. Complete the Perspective Risk associations to define which perspectives are associated to which risk records. Use the worksheet IDs assigned to the rows in the PerspectiveItem and Risk worksheets.
    f. Complete the Perspective Control associations to define which perspectives are associated to which control records. Use the worksheet IDs assigned to the rows in the PerspectiveItem and Control worksheets.
    g. Run the import. Specify Incremental Load.
    h. Verify that the data was loaded correctly before proceeding to import the next set of data.

# 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

# 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 value, 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.

## Finding 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?

# Disabling 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.