Oracle® Enterprise Governance, Risk and Compliance Manager

User Guide

Release 8.6.4

Part No. E23925-01

November 2011

ORACLE

Oracle Enterprise Governance, Risk and Compliance Manager User Guide

Part No. E23925-01

Contents

7 Issue Management

8 Managing Assessments

9 Managing Surveys

Preface

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

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

About Enterprise Governance, Risk and Compliance Manager

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.

Objects Explained

Objects are reusable, fundamental building blocks that describe common core objects such as risks or controls. There are also base objects, which are general-purpose objects that are used as defined in the module template. For example, in the Financial Governance module template, a base object is defined as Process. When included in a business model, objects support specific GRC initiatives, such as financial compliance.

- The type and number of objects that you can use are defined by the template used when you create a module.
- User-defined attributes can extend objects.
- Changes to objects are tracked through revisions.

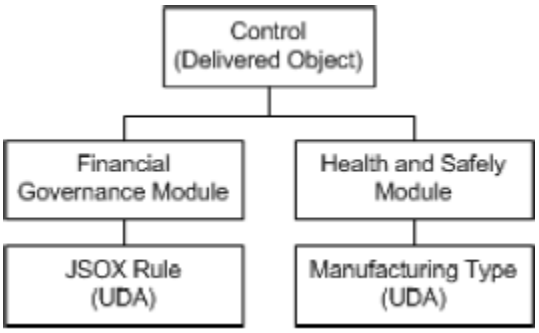
What Are User-Defined Attributes?

Occasionally you might need to specify additional information for an object, the better to suit your requirements and to illustrate objects within your organization. To accomplish this, you can create user-defined attributes (UDA) to provide additional classification or other clarifying information specific to your business. UDAs:

- Are retained when you upgrade or update your system.
- Support basic validation based on data type.
- Are translatable.

Example: Using UDAs

In this example, a control is a delivered object that exists in two modules, the delivered Financial Governance module and a user-created module called Health and Safety. Based on this module configuration, the Control Object can have UDAs for JSOX rules for the Financial Governance module, and for the Health and Safety module, the Control UDA can be for manufacturing type.



Perspectives Explained

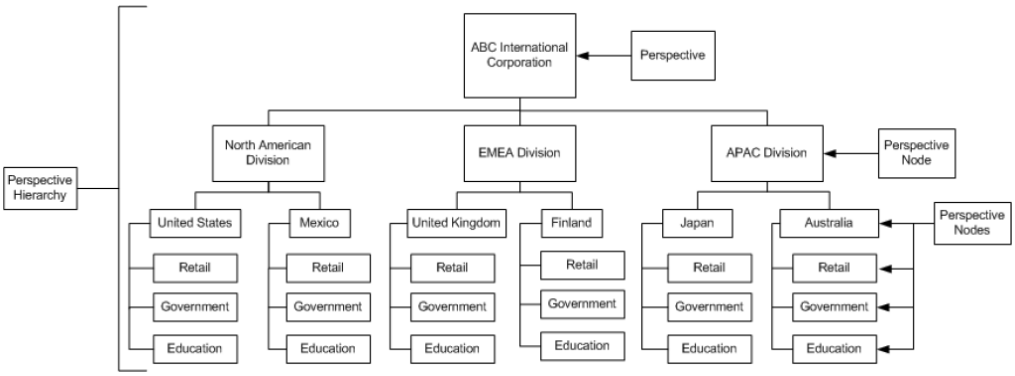
Perspectives provide hierarchical shape, structure, and organization for core objects such as risks, controls, and base objects. They also support key user activities such as analytics and reporting. Perspective management provides a centralized interface for you to define different views into the GRC data.

Perspectives contain the following elements:

- Perspective value: The element that is associated to an object.
- Hierarchy: The structure or arrangement of the perspectives.

The perspective hierarchy describes the structure and the relationships between the perspectives. This enables perspective values to be in multiple hierarchies.

The following is an example of a corporate structure perspective hierarchy:



For more information, refer to "Perspective Management" (page 3-1).

Perspectives are not required unless specified within the module configuration. Refer to "Managing Module Perspectives" (page 13-5) for details. At least one perspective is needed for the object to be controlled through data-level security. Refer to "Managing Data Roles" (page 12-2) for information on using perspectives to manage security.

Risks Explained

A risk is defined as the chance of an event occurring that will have a positive or negative impact on the objectives of the organization or a division. Refer to "Risk Management Explained" (page 4-1) for details of managing risks.

An event is the occurrence of a particular set of circumstances, which can be certain or uncertain and can be a single occurrence or a series of occurrences.

A consequence is the outcome or impact of an event. An event can have more than one consequence, which can range from positive to negative. Consequences:

- Can be expressed qualitatively or quantitatively.
- Are considered in relation to the achievement of the objectives.

Controls Explained

A control is an existing process, policy, device, practice, or other action that minimizes negative risk or enhances positive opportunities.

Issues Explained

Issues are reported defects or deficiencies against any object or its related activities, such as its assessments. Issues:

- Can be associated with any object (risk, control, or other base object).
- Are assigned to users based on their job roles.
- Are reviewed for validation and disposition, which may require remediation.

Issues typically have a shorter life cycle than risks and controls. Risks and controls tend to be more enduring, given the nature of the enterprise's strategy as well as the market and geographic segments in which an enterprise operates.

Remediation is the process of correcting or addressing an issue. A remediation plan is the documented response actions for an issue and is the way progress on the resolution of the issue is tracked.

Assessments Explained

A business process and its risks and controls require periodic review of how they are defined and implemented to ensure that the appropriate level of documentation and control is in place. An assessment evaluates the validity and effectiveness of controls, risks, and the business process to find out if any element is missing or out of place, or has changed. You can perform assessments on a single or multiple risks or controls, a combination of risks and controls, base objects, and perspectives.

Surveys Explained

You can create surveys to be used within different aspects of the system — for example, assessment certifications, evidence gathering, or testing. You can manage questions and forms to enable the reuse of these survey elements. Survey responses are captured and can be used in multiple ways.

Surveys are based on survey templates. A survey template is a collection of questions that enable the survey to be reused. The template also provides the ability to include surveys within an assessment.

Application Modules Explained

An application module is a collection of objects (for example, risk, control, or base object) configured to depict the underlying information model of the GRC solution, such as a financial compliance model. Application modules:

- Are based on a template that identifies the set of objects that are necessary to satisfy a specific GRC business initiative (for example, process, risk and control object types that are necessary to address a financial compliance initiative).
- Define the process flows required for the application module to enable the specific GRC business initiative.
- Can be prepopulated with content specific to the business initiative.

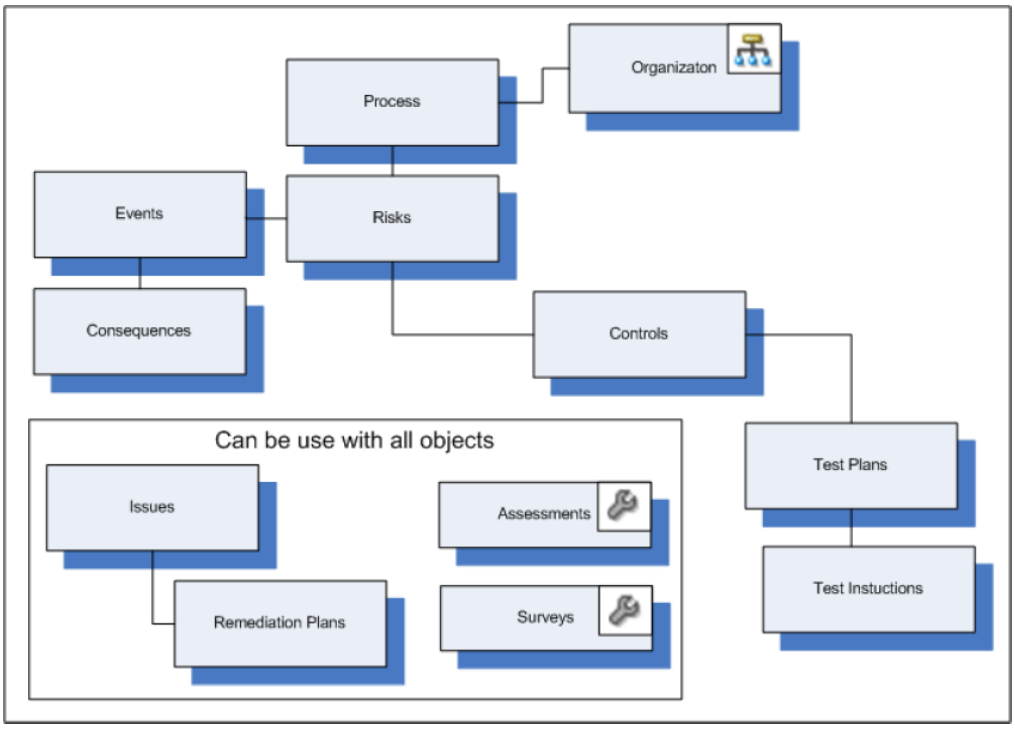
The objects available for use in an application module depend on the template used to create the module. Objects are configured to identify options appropriate for a specific module. See "Managing Modules" (page 13-1) for information on configuration.

What Is the Financial Governance Module?

The Financial Governance module is a delivered module that addresses financial reporting mandates. It includes the following objects:

- Process: This is a base object defined for use as a process. Refer to “Managing Base Objects” (page 6-1) for details on managing base objects.
- Risk
- Event
- Consequence
- Control
- Issue
- Perspective

Graphically, the Financial Governance module can be represented as follows:



Reporting Explained

There are two ways to access reports in EGRCM:

- From the Navigation menu, choose Report Management. From there you can run defined reports for assessments, issues, controls, risks, security, and administration. Refer to “Reporting” (page 10-1) for additional information.
- From any object-overview page, choose the Analytics tab to view reports and graphs. You can drill into these for additional details.

2

Basic Application Operation and Common Tasks

Security Overview

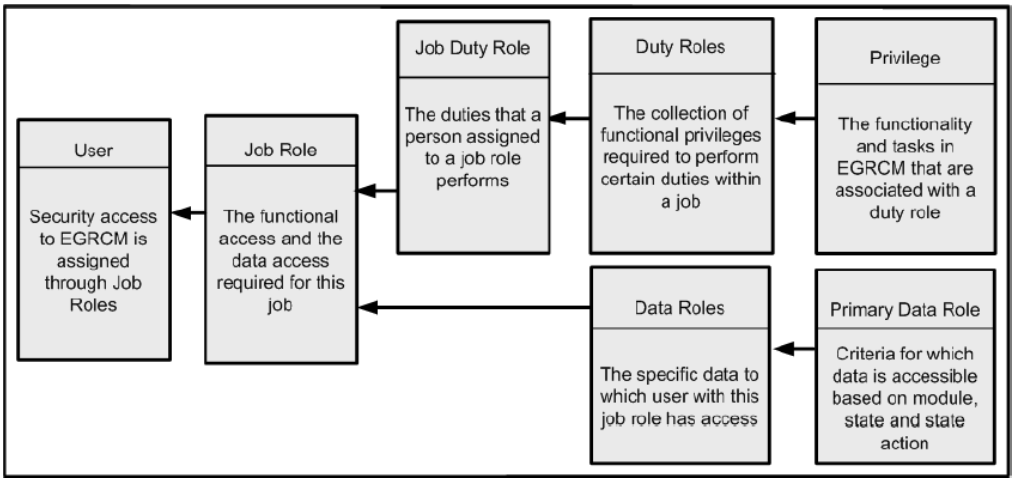
Each user is required to provide a user ID and password to log in to the application. This allows each user access only to assigned functions and content. Functions a user is not authorized to access do not appear in the interface for that user's account.

Users with security-administration privileges, such as Security Administrators, set up user accounts. The Security Administrator also assigns one or more roles to each user, based on the need to work with content and to track activity for compliance.

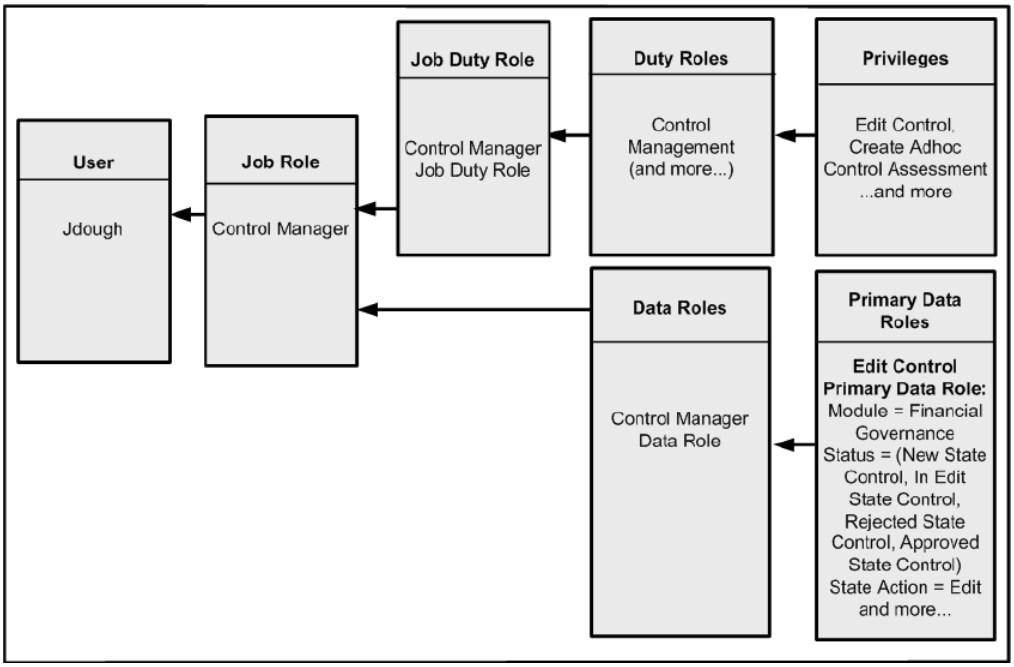
Roles Explained

Each user is assigned specific job roles, which allows him to perform only those tasks that are appropriate to his job. This provides security, as only users assigned certain roles are allowed to perform certain tasks and to access certain data. Security Administrators can create new duty, job, and data roles as needed. Refer to "Managing Security" (page 12-1) for details of user and role creation.

Each job role is associated to duty roles and data roles, which provide discrete privileges in the application. Security Administrators can create new duty and data roles as needed. Access to functionality is determined by duty roles, and access to data is determined by data roles, as follows:



The following example shows a user whose ID is “jdough,” and her functional and data roles as a Control Manager:



Basic User Interface

The tasks you see listed on the Navigator and what you see on your dashboards are determined by the roles and privileges that have been granted to you by your Security Administrator. In addition, your GRC Administrator can configure the system to hide functions that are not relevant to your business process.

Home Page Explained

Your home page is your default landing page. It shows your worklist, watchlist, and notifications. It displays:

- My Watchlist: The watchlist is a categorized summary of your worklist entries. Within the categories, they are summarized and grouped by activity type. When you select a certain watchlist grouping, the appropriate work area for that category is displayed, and only that group of watchlist items is displayed within the worklist. This narrows down your pending work and brings into focus the work you have selected.
- Pending Activities: These include:
  - Worklists: This displays worklist entries accessible to users with your job role for the current work area.

    If your Administrator has chosen to implement it, you will receive email messages at specified intervals. Each message contains a summary of your outstanding worklist entries, with links to appropriate EGRCM pages in which to complete tasks.

– Notifications: This displays a list of changes (including reviews and approvals) to objects related to objects to which you have access. For example, if you have access to Risk ABC and it is related to Control X, when a change to Control X is approved, you are notified. You also receive notification of completed activities, such as if Risk ABC is analyzed or evaluated.

Common Regions on Overview Pages

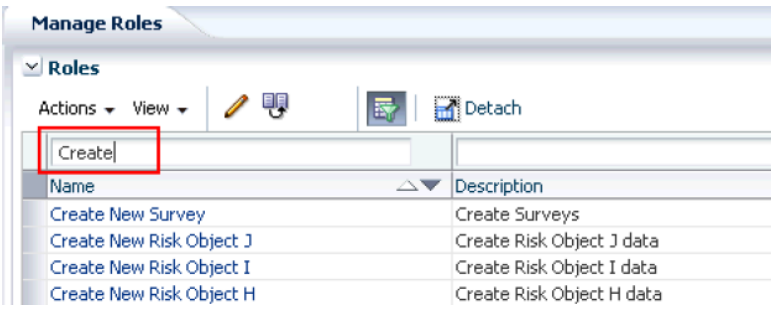
In addition to the Pending Activities region shown on your home page, most overview pages also contain the following regions:

- Objects listing: This displays active objects to which you have access. (You might have privileges to view only certain objects. You can modify those objects only if you have appropriate additional privileges to do so.) An Objects listing also provides a centralized launching pad into key tasks and work areas, and provides a way to monitor the status of underlying transactions.
- Tasks: This lists all tasks that you can perform from the current page.
- Search: Depending on the page you are viewing, you can search by name, description, ID, status, or method.
- Favorites: This displays objects you have designated as your favorites — typically, those you use frequently.
- Analytics tab: This displays graphs that complement the business process. They answer fundamental questions about the health of the business — financial, operational, or comparative in nature.

Common Elements in Overview, Dashboard, and Component Pages

Common elements in dashboards include:

- Linked object names: These enable you to perform management tasks for objects that are accessible to you.
- Bars or pie slices in graphs: Mouse over any of these to view details of the item it represents, or click on it to drill to secondary pages that provide more details.
- Filters: These enable you to limit the data you are viewing in the current chart or graph. In many tables, you can filter by date or status.
- Date slider: This enables you to modify the date range displayed in a chart.
- Query by Example: This allows you to limit lists of values based on an example you provide. Below, for example, a user chooses to see only values containing the word *Create*.



Action icons provide shortcuts to actions you can perform:

 Create a new object.

 Edit the current object.

 Delete a selected object (for example, on an overview page). Or remove the association between a selected object and the current object. For example, if you delete a control from the Related Controls region, the control remains in the database, but is no longer associated with the current object.

 Write a description, which is limited to two thousand characters.

 Make a copy of the current object, which you can then edit.

 Add an existing object to the current field, or add a new row to a table.

Assessment Result icons graphically depict assessment results. For example:

 Depending on the object that was assessed, this can indicate Pass, I agree, Completed, or Meets guidance.

 Depending on the object that was assessed, this can indicate Pass with noted exceptions, I agree with noted exceptions, Requires documentation, Requires additional analysis, or Requires evaluation.

 Depending on the object that was assessed, this can indicate Failed, I do not agree, or Out of tolerance.

 Indicates the assessor had no opinion.

 Indicates that no action is needed.

 Indicates that an assessment has not been started.

Object States

The following list shows states in which you might see an object, depending on your business processes and the object. For example, In Review or Awaiting Approval might not be required in your workflow.

- New: The object has been created and saved.
- In Edit: The object has been modified and saved but not submitted.
- Reported: The object has been submitted for validation (proposed risk and issues only).
- In Review: The object has been submitted and is awaiting review.
- Request for Information in Review: During review, the reviewer has asked for more information.
- Awaiting Approval: The object has been reviewed and awaits approval.
- Request for Information in Approval: During approval, the approver has asked for more information.

- Rejected: The object was rejected during the review or approval process.
- Approved: Approved.
- Completed Review: A remediation is completed and is in review (remediation plan only).
- Completed Additional Information in Review: A completed remediation is in review and the reviewer has asked for more information (remediation plan only).
- Completed Additional Information in Approval: A completed remediation is at the approval step, and the approver has asked for more information (remediation plan only).
- Closed in Review: An issue is closed and is in review (issue only).
- Closed Approve: Review is completed for a closed issue, and the issue now awaits approval (issue only).
- Closed Additional Information in Review: A closed issue is in review, and the reviewer has asked for more information (issue only).
- Closed Additional Information in Approval: A closed issue is at the approval step, and the approver has asked for more information (issue only).
- Closed: Closed.

Objects can also be in one of two statuses, Active and Inactive.

Common Tasks

The following tasks are common to most components:

- Setting preferences.
- Working with attachments.
- Working with revisions.
- Managing objects.
- Creating issues for objects.

Preferences Explained

You can set the following personal options by selecting Preferences from the link on your home page:

- The Details section includes details about the user, including personal information such as first, middle, and last names, phone numbers, addresses and email addresses. Although you can specify two email addresses, notifications are sent only to email address 1. Email address 2 is used only for documentation purposes.
- The Regional section allows you to set your territory, time zone, time and number format, and language.
- The Assigned Roles section displays all the roles currently assigned to you.

Attachments Explained

Attachments are supporting documents associated with components. You can attach documents in many formats, including URL references, documents produced from many popular software applications, or other formats available to an organization. Attachment examples include business process narratives, business process flow charts, control test instructions, and supporting issue remediation documentation.

When you specify an attachment, you must choose the following:

- The type of attachment, either Desktop File (a file located on your PC) or URL (a link to a web site).
- A file name or URL. If you enter a URL, it must be fully qualified, for example http://www.oracle.com.
- The content type. This is a description of the content of the attachment. Some content types are seeded; your GRC Administrator can create other content types via the Setup and Administration Manage Content Types menu.
- Title: Enter a title for the attachment. The title defaults to the file name, but you can change it if you desire.

Revisions Explained

A new revision is created every time a component in the Active or Approved state is created or changed. This provides an automatic audit log to the changes related to the component. The revision date is automatically set to the system date and cannot be changed. You can compare across multiple revisions, print, and export the comparison results.

You can view a Revision History report for some objects. The report typically displays:

- The revision number.
- The names of any attributes changed in that revision.
- The old and new values for each changed attribute.
- The name of the user who modified the object.
- The date on which the modification was made.

Managing Objects Explained

Most objects have a page from which you can view and manage objects. Managing objects consists of many tasks, and the tasks that are available to you depend on your role. For example, if you have the privileges only to review control changes, when you open a control on the Manage Control page, you will not be able to edit the control definition.

Copying Objects Explained

The copy functionality enables you to create separate and distinct replicas of objects in the application. You can copy the following:

- Objects
  - Risks
  - Controls
  - Remediation plans
  - Perspective hierarchies

    Note: Copying perspective hierarchies does not create copies of the individual values in the perspective library; it reuses the existing perspective values.
  - Survey templates
  - Survey choice sets
  - Survey questions
- Security artifacts
  - Users
  - Data roles
  - Duty roles
  - Job roles

When a copy of an object is created, the following associated items are not copied into the new object:

- Attachments
- Comments
- Relationships to issues
- Transactions such as assessments, analyses, evaluations, test results, and action items

To copy an object:

1. Navigate to the overview or manage page for the object you wish to copy. For example, in the Financial Governance module, you might select the Control Management page.
2. Select an object from the overview or manage page.
3. Select Copy from the Actions menu, or select the Copy icon. The Create page is invoked, with values entered in all fields except the name.
4. Enter a new name for the copy of the object. This is a required field; you must assign a unique name to the copy.
5. Enter any other changes you wish to make.
6. When prompted, choose one of the following:
   - Save: Saves the new object and leaves the page open for further editing.
   - Save and Close: Saves the new object and closes the page. You can continue editing the new object at a later time.
   - Save and Submit: Saves the new object and places it into the workflow for any review and approvals as specified in the object definition.

Reviewing Objects Explained

When an object is in the In Review state and you have the appropriate job role to review that object, the review task appears on your worklist. To review an object, select it and click the edit button. You have the following options:

- Accept the object as is. Once the review is complete, if an approval is required, the approval task appears on the worklist of appropriate users. If approval is not required, the object's state is set to Approved. For a list of states and their meanings, refer to "Object States" (page 2-4).
- Request information. The object remains in the In Review state and a new entry appears on the appropriate users' worklists, notifying them that more information is requested by a reviewer or approver. Another reviewer can still complete his review while the first reviewer waits for information.
- Reject the object. This removes the object from the workflow and the user who submitted the change is notified.
- Cancel your review. This leaves the object in its current state, unchanged.

Approving Objects Explained

If an object awaits approval and you have the appropriate job role to approve that object, the approval task appears on your worklist. To approve an object, select it and click the edit button. You have the following options:

- Approve the object as is. The object is placed into the Approved state. For a list of states and their meanings, refer to "Object States" (page 2-4).
- Request information. The object remains in review, and a new entry appears on the worklist of the user who submitted the change, notifying her that more information is requested by a reviewer or approver. Another reviewer can still complete his review while the first reviewer awaits information.
- Reject the object. This removes the object from the workflow, and the user who submitted the change is notified.
- Cancel your review. This leaves the object in its current state, unchanged.

Creating Issues: Critical Choices

Issues are defects or deficiencies that are detected for an object. Although you can create issues from within Issue Management, doing so is limited to only those roles that have access to Issue Management. You will usually create issues directly in the object. When creating an issue for an object, in addition to specifying a name and description, you also need to specify the severity of the issue. For example, is it a significant defect, a minor gap in functionality, or is it an issue that can be fixed with improved documentation? If you create the issue from Issue Management, you must also specify the object with which the issue is associated.

EGRCM Reporting Described

Run embedded reports from the Report Management link. Refer to "Reporting" (page 10-1) for details.

3

Perspective Management

Perspective Management Explained

Managing a perspective can entail:

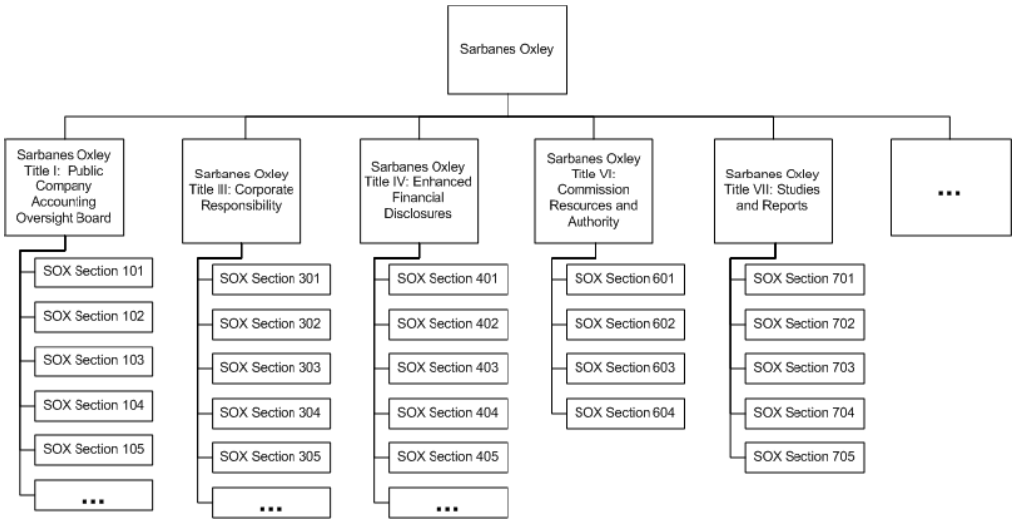
- Creating new perspectives, or editing existing perspectives. For example, a perspective called Organization is seeded in the application, but is empty and must be populated with values and hierarchy.
- Duplicating an existing perspective.
- Creating an issue (page 2-8).
- Creating assessments to certify perspectives.
- Completing assessments to certify perspectives. For example, in the Financial Governance module, you might perform certification for the organization perspective, which includes reviewing the processes, risks, and controls within the organization.
- Retiring or reactivating a hierarchy.

Delivered Perspectives Explained

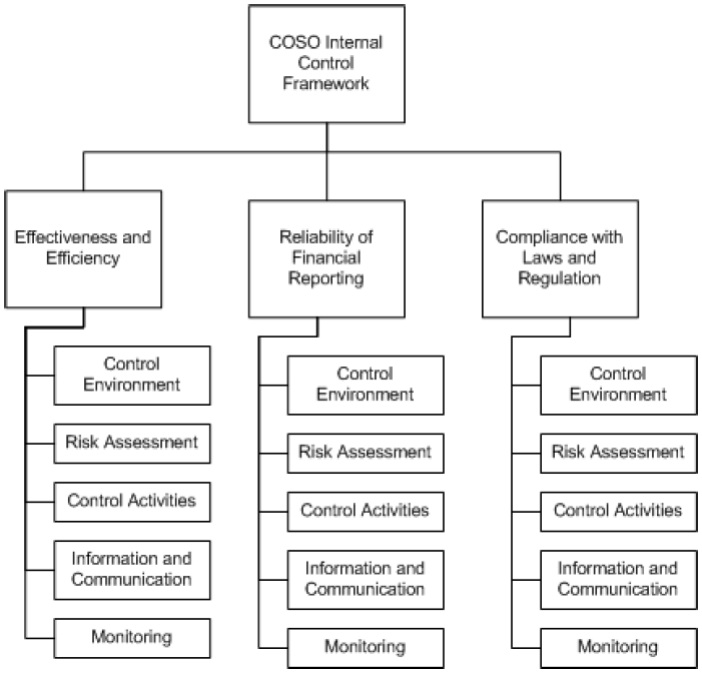
A perspective is a depiction of the hierarchical relationship between units such as corporate divisions, standards and frameworks, projects, financial compliance accounts, risk catalog, and so forth. Before creating a new perspective, consider the type of perspective that you need to create. In the Financial Governance module, there are five delivered perspective types:

- Organization describes the internal structure of a business. It is empty by default, and you must populate it to describe your organization. For additional details on populating a perspective, refer to "Creating Perspectives: Critical Choices" (page 3-3).
- Financial Governance Accounts is a delivered perspective, but it does not contain any values. You can add accounts to fit your business needs.
- The Major Process perspective hierarchy does not contain any values as that depends on how your company is structured.

- A Laws and Regulations perspective describes Sarbanes Oxley regulations. You can create other laws and regulations perspectives as needed.



- A Standard and Framework perspective describes the COSO Internal Control Framework. You can create others as needed.



After you have selected a type, you can populate the perspective by adding values.

When Should I Create an Issue for a Perspective?

Create an issue when you need to document any potential events that might affect the perspective. For example, you might create an issue on an Organization perspective if a department is missing or in the wrong place in the hierarchy. For additional information about issues, refer to “Creating Issues: Critical Choices” (page 2-8).

Creating Perspectives: Critical Choices

The basic process for creating a perspective is:

1. Determine which type of perspective you need to create.
2. Create or add values to the hierarchy.
3. Depending on your process, submit your perspective for review or approval.
4. As required, create an assessment to have your perspective certified.

When building the perspective, you indicate which values belong at the various levels within the hierarchy. The highest level within the hierarchy is called the root. Each value within the hierarchy structure is called a node. A node is a perspective value. Add a node to the hierarchy by selecting either the Create or Add icon. Once you have created the new node, you can change its position in the hierarchy by increasing or decreasing its indenting or using the up and down arrows.

Perspective Assessments Explained

Create a certification assessment for a perspective when you need to certify the perspective. There are two methods of initiating assessments:

- Create an ad hoc assessment (page 8-3) from the Manage Perspectives page.
- Navigate to Assessment Management and:
    1. Create an assessment template (page 8-4).
    2. Create an assessment plan (page 8-5).
    3. Initiate the assessment (page 8-5).

Perspective Certification Process Explained

Perspective certification is performed from the bottom up. The users assigned to perform the assessment at the lowest level of the hierarchy are notified via a work-list item. When all assessment tasks are completed for all child nodes of a parent node, then the system generates a worklist for the next level up in the hierarchy. Assessors receive a worklist item only when it is appropriate for them to complete their activities within the hierarchy.

A parent node cannot be certified until all its subordinates have been certified. The certification process is:

1. A user (usually the Perspective Manager) creates an assessment to certify the perspective hierarchy.
2. A worklist entry is sent to users who have the appropriate roles to perform the certification activity for the lowest level within the hierarchy. The certification process controls when it is appropriate for the assessors at each level to complete the certification. The status of the certification results at this time is Not Started.

   Tip: On the Certify Perspective page, only certify actions for the perspectives that you own, and for which already-certified subordinate perspectives are

displayed. All subordinate perspectives must have the certification completed before the next level in the perspective hierarchy can be certified.

3. When all child nodes within a branch have the lowest-level nodes certified, the process moves up to the next level within the hierarchy. The assessors responsible for those items receive worklist entries to perform the certification activity.
4. The process continues until the root node is certified. The certification of the root node is the certification of the hierarchy. The certification is complete when the root node is certified.

Note: Perspective assessment is limited to the certify activity type; it does not use the standard complete assessment page. Unlike other object assessments, perspective assessments do not go through review and approval cycles. Once the root node is certified, the assessment is complete and can be closed.

4

Risk Management

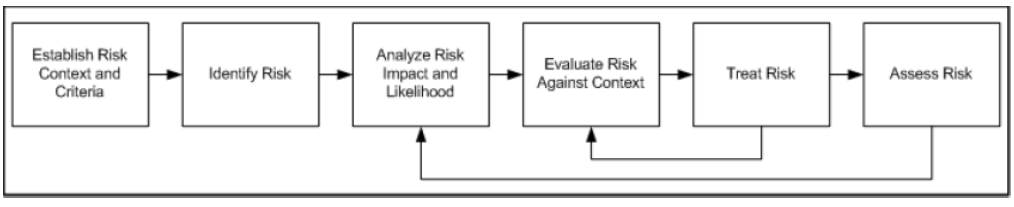
Risk Management Explained

Risk management includes the following tasks:

- Viewing metrics on the Risk Overview Analytics tab. Metrics can include risks by context, tolerance, significance, and other reports.
- Proposing a risk.
- Creating a risk.
- Creating an event.
- Creating a consequence.
- Performing risk analysis.
- Evaluating a risk.
- Treating a risk.
- Assessing a risk.
- Performing risk administration tasks.
- Creating issues for risks (page 2-8).
- Managing risk revisions (page 2-6).

Risk Life Cycle Explained

Risk management provides a comprehensive set of information models and capabilities necessary to define and manage the needs of a sophisticated risk management practice. The process of risk management comprises:



- Risk Context: The risk context defines the general parameters for how risks must be managed and the scope for the enterprise risk management process. The

risk context should include the organization's external and internal environment and the purpose of the risk management activities. For example, when an organization defines its risk context, it should establish its overall strategies, objectives, goals, scope and the understanding of the parameters for the risk activities.

- Risk Identification: Determining risk classification and associations.
- Risk Analysis: Understanding the nature, and deducing the level, of risk.
- Risk Evaluation: Comparing the level of the risk against risk criteria. The risk criteria are the terms of reference by which the significance of risk is assessed. Risk criteria can include associated cost and benefits, legal and statutory requirements, socioeconomic and environmental aspects, the concerns of stakeholders, priorities, and other inputs to the assessment. The risk context is used when evaluating the risk.
- Risk Treatment: Selecting and implementing a method of addressing the risk with a goal of minimizing the risk's negative consequences.
- Risk Assessment: Appraising the risk definition and evaluating the systems and business processes they support. Assessment types include certification and audit.

Proposing a Risk Explained

A proposed risk is a risk candidate; it may or may not become a formalized risk, depending on whether the risk is relevant or significant to the risk context. A proposed risk may also be a duplicate of a known risk. When proposing a risk, you should specify:

- What event would cause this risk? How, when, and where would this happen? How likely is it to happen?
- If this risk were to occur, what would be the consequence?

Once the proposed risk is submitted, it is put into Reported state for a risk manager to review. If the risk manager approves the risk, she then creates the new risk, and it is entered into the risk workflow.

What Is the Difference Between Creating and Proposing a Risk?

Any user who has the appropriate role can propose a risk. A proposed risk must be approved by a user who has the Validate Proposed Risk privilege. Risks can only be created by users who have been given access to risk functionality. The Propose Risk task is also available on the dashboard for users who do not have access to the risk work area, but do have access to the Propose Risk functionality. Once a risk is created, it follows the regular risk workflow.

Do I Always Have to Propose a Risk Before I Can Create One?

No, risks do not have to be proposed before they are created. For example, you do not have to propose a known risk, you can just create it, provided you have the appropriate privileges to create a new risk.

Are Risks Automatically Created from Proposed Risks?

No. If a user with the appropriate role (for example, a Risk Manager) decides that a proposed risk is valid, that user manually creates the new risk. Not all proposed risks become actual risks; that is up to the discretion of the Risk Manager. A proposed risk, once submitted, is not deleted, even if it does not become a formal risk.

Creating a New Risk: Critical Choices

When creating a risk, consider:

- The context for the risk:
  - Set risk criteria and weighting against corporate performance objectives.
  - Set tolerance thresholds and significance scales.

  Risk appetite is the level of risk that is acceptable in order to gain benefit. In the delivered Financial Governance module, there is one seeded context called Financial Governance Context. It uses the Financial Governance Significance Model to define the risk appetite. The risk criteria for the Financial Governance Significance Model is measured in terms of effectiveness, reliability, and compliance.

  You may also have other contexts available that use other models as defined for your business by your GRC Administrator.
- The analysis model that will be used with the risk. In the delivered Financial Governance module, there is one analysis model called Financial Governance.
- The form of currency in which the risk will be measured.
- Additional details required by your business process.

  If your GRC Administrator has added user-defined attributes (UDAs) to your risk definition, they will appear in this section.
- Any events or consequences associated with the risk. Determine if you need to associate any events or consequences to your risk.

Editing Related Controls: Critical Choices

When editing related controls for a risk, you should consider the following:

- What is the likelihood that the risk will occur?
- What do you expect the residual impact to be?
- What primary control do you want to include?
- What subordinate control do you want to include? This control will be subordinate to the primary control.
- What stratification should be assigned to the related control? Control stratification is the classification of a control-to-control relationship that can enhance the management of risk mitigation. Options for stratification are:
  - Key: A control that is of significant importance to the proper operation of a business process. A monitoring or subordinate control can be related to a key control. A key control does not have a subclass and cannot be related to a secondary control or to another key control.

- Monitoring: A control that monitors one or more related controls. It is used for management assessment, for example assessing a monitoring control and not assessing its related key control or related secondary control. A monitoring control cannot be related to a subordinate control or to another monitoring control.
- Compensating: Controls institute additional controls to accept the risk inherent with the control weakness. The control does not duplicate its primary control. It provides coverage of some aspects of the control (assuming management approval).
- Redundant: Controls that institute the same controls as the key control.
- Mitigating: Controls that are currently eliminating risk for a process.

Creating a New Event: Critical Choices

An event is a particular set of circumstances that may or may not occur, and can be a single occurrence or a series of occurrences. When creating a new event, you must decide:

- What likelihood model is most appropriate for this event? The default likelihood model is qualitative, but your GRC Administrator can define other models.
- What is the likelihood that this event will occur? The values that you can select are determined by the likelihood model you choose.
- What are consequences of this event occurring? Select an consequence that describes the possible outcome or impact of the event. You can associate more than one consequence. The possibilities can be positive or negative, and can be expressed qualitatively or quantitatively.

Creating New Consequences: Critical Choices

A consequence is the outcome or impact of an event. When defining a consequence, you should consider:

- What impact model is appropriate for this consequence? The impact model contains the criteria for weighting the importance of the event consequence to the risk in the case the event occurred. The default impact model is qualitative, but your GRC Administrator can create other models.
- If this even occurs, what could the negative or positive outcome be to the business objectives? The options you can select change based on the impact model you select.

Risk Analysis Explained

Risk analysis enables you to develop an understanding of the risks that may impact your business. The risk analysis process defines a structure whereby your organization can provide input to decisions on whether risks need to be treated and apply the most suitable and cost-effective risk treatment strategies.

Risk analysis involves consideration of multiple sources: the actual risk, factors of the consequences (positive and negative), and the likelihood of the consequences occurring. Various degrees of risk analysis can be performed. The degree of detail depends on that risk, the purpose of the analysis itself, and is based on the information, data, and resources that are available.

Risk analysis is the systematic process to understand the nature of the risk level, and to determine ways to reduce it. The objective is to:

- Transform risk data into decision-making information.
- Evaluate impact, probability, and time frame.
- Classify and prioritize risks.

Risk analysis can provide a basis for risk evaluation and decisions about risk treatment. There are two types of risk analysis:

- Qualitative: The process of examining risk characteristics by description rather than numerical criteria. Qualitative analysis can be performed as an initial analysis of risk prior to further detailed analysis.
- Quantitative: Associates numeric values to qualitative likelihood and impact scales.

Risk Analysis Process

The risk analysis process is:

1. Define and manage the risk analysis models and the analysis formulas to be used within a risk analysis activity. See "Risk Administration" (page 4-8) for details on creating models.
2. Define risk formulas by utilizing formulas that are available in the system.
3. Create the risk analysis.
4. A user with the appropriate job role analyzes the risk level.
5. A user with the appropriate job role marks the analysis complete. The analysis cannot be changed after it is complete.

Create an Analysis: Critical Choices

When creating a risk analysis, you must make critical choices regarding the model that will be used for analysis:

- Which likelihood model is appropriate for this analysis?

  Risk analysis models provide definitions of risk formulas and add dimension to the risk analysis. The likelihood model contains the description or numeric weight of the probability of frequency to be applied to a risk during analysis. The Financial Governance module includes a delivered qualitative likelihood model, and you can create your own additional models.

- Which risk likelihood is appropriate for this analysis?

  The available risk likelihood options are determined by the likelihood model you specify.

- Which impact model is appropriate?

  The impact model contains the criteria for weighting the significance of the event's consequences if the event were actually to occur. Select the model you want to use. The Financial Governance module includes a delivered qualitative impact model, and you can also create your own impact models.

- What is the potential impact of this risk?

  Options change based on which impact model you specify. You can only associate impact models that are the same type as the impact model type.

See also "Risk Administration" on page 4-8.

Risk Evaluation Explained

Risk evaluation is the activity of evaluating a risk in the parameters of the risk context definition, to determine if treatment is required. Within the risk context definition, a tolerance model is associated to the context, which is utilized during the risk evaluation activity. During the evaluation, a rating is associated to the criteria, which provides the context for determining if treatment is required. You can prioritize the criteria requiring treatment based on a scale of 1 to 100.

You can perform risk evaluations only after the risk context and risk criteria are associated to a risk. You may also perform risk analysis first, but this is not necessary. You can perform multiple risk evaluations. You typically perform risk evaluation after the risk criteria have been modified, risk analysis has been modified, or on a scheduled time interval. The appropriate user is notified when a risk has been modified and that user can decide if an evaluation is appropriate.

Creating an Evaluation: Critical Choices

When creating an evaluation, consider the following:

- How serious is the nature of this risk? Selecting the Catastrophic check box sets the risk rating to the maximum setting of 100.
- What are the criteria values for this risk? Enter tolerance scores for each criterion.

Risk Assessments Explained

Perform an assessment to evaluate the validity and effectiveness of a risk. There are two methods of performing assessments:

- Create an ad hoc assessment (page 8-3) from the Assessment tab of a risk.
- Navigate to Assessment Management and:
  1. Create an assessment template (page 8-4).
  2. Create an assessment plan (page 8-5).
  3. Initiate the assessment (page 8-5).

For related information, see "Completing Assessments Explained" (page 8-6).

Risk Treatments Explained

Creating a New Treatment Plan: Critical Choices

When creating a new treatment plan, you should consider the following:

- How will the treatment plan be used?
  - In Use: Indicates that the treatment is currently being used to reduce risk.
  - Target: Indicates a long-range treatment that will eventually reduce risk. For example if the risk is "Lawsuits from environmental hazards," a target treatment might be "Reduce emissions at all business centers by 30 percent."
- What, if any, treatments should be performed? A treatment plan identifies, evaluates, and implements options for treating risks.
- What are the residual likelihood and impact of the treatment plan? When one or more control components are associated with a risk, and the control has the risk impact capability enabled, residual (controlled) risk values are calculated from the sum of the related control impact values.

Creating a New Treatment: Critical Choices

Create a risk treatment to identify options for treating risks, evaluating those options, preparing treatment plans, and implementing them. Selecting the best option involves balancing the costs of implementing each option against the benefits derived from it. In general, the cost of managing risks needs to be commensurate with the benefits obtained. The purpose of treatment plans is to document how chosen options are to be implemented.

When creating a new treatment, you must make the following decisions:

- What type of treatment are you creating? Types of treatment are:
  - Avoid: A decision not to become involved in a risk situation, or an action to withdraw from it.
  - Reduction: Actions taken to lessen the probability of a risk, its negative consequences, or both.
  - Retained: Acceptance of burden of loss, or benefit of gain, from a particular risk. Risk retention includes the acceptance of risks that have not been identified. Risk retention does not include treatments involving insurance, or transfer by other means.
  - Shared: Sharing with another party the burden of loss or benefit of gain for a risk.
- What is the estimated cost of performing this treatment? This cost may be linked to the cost of the controls that are associated with a treatment or a user-entered value.
- Link Treatment Cost to Control Cost: Select this option if you want to link the cost of the treatment to the cost of the related control. If you select this, the control cost will override any value you have entered in the Treatment Cost field.

See also, "Editing Related Controls: Critical Choices" (page 4-3).

Risk Administration

Creating an Analysis Model: Critical Choices

A risk analysis model describes the method to determine the impact of risk uncertainty. When creating an analysis model, you should consider:

- What type of analysis will be performed? Choose qualitative or quantitative.
- What likelihood model should be used? The options you see here are based on the analysis type you choose.
- What impact model should be used?
  - For qualitative models, what are the appropriate risk levels? You must specify the low and high values, and a label for the risk level. For example, 1–10 might be "Low," 11–90 "Medium," and 91–100 "High."
  - For quantitative models, what risk level formula should be used? Risk level mapping values map the likelihood and impact values to generate the risk level output. The formulas are:

    Product: The only type that can be used for qualitative analysis. When you select qualitative and the analysis type, the risk level formula defaults to Product. The risk level formula for Product is Likelihood × Impact.

    Weighted: Available only for quantitative analysis. The formula is Risk Level = (Impact × Weighting Factor)^{X} × Likelihood ^{Y}, where you supply the Weighting Factor, power X, and power Y.

Creating a Likelihood or Impact Model: Critical Choices

A likelihood model assigns labels to the chance that a potential risk will actually occur. An impact model contains criteria to weigh the significance of the event consequence in relation to the risk, should the event occur.

When creating either type of model, consider the following:

- What type of model should be used? Choose qualitative or semi-qualitative.
- For qualitative models, what labels and ratings are appropriate? For example:

Label	Rating
Low	1
Medium	3
High	5

- For semi-qualitative models, what low and high values and labels are appropriate? For example:

Label	Low Value	High Value
Low	1	2
Medium	3	4
High	5	6

Creating a Risk Context Model: Critical Decisions

The risk context model defines how the risk-rating and risk-significance values are derived during risk evaluation. When creating a risk context model, consider:

- Which risk significance model should be used? The risk significance model determines the risk significance value; it uses the overall risk rating from the risk evaluation activity. The risk significance model uses a risk rating minimum and risk rating maximum range to determine the risk significance value.
- What is the appropriate risk context criteria? This is a user-defined value that is used by the risk context model. After you define the risk criteria value it can be selected by the risk context model.
- What details are required for the model? You can include:
  - Value: Values can be either strings (such as *High*, *Medium*, and *Low*) or integers (1–9).
  - Tolerance: Risk tolerance is the acceptable level or risk when compared to the possible benefits. Options for risk tolerance are *Accept*, *Monitor*, and *Treat*.
  - Rating: The rating is the tolerance score and can be any number from 1 to 100.

For example, you might create a risk context with a criterion named Compliance, and the following details:

Label	Tolerance	Rating
1	Accept	10
2	Monitor	30
3	Monitor	50
4	Treat	20
5	Treat	100

Risk Significance Models Explained

The risk significance model determines the risk significance value using the overall risk rating from the risk-evaluation activity. The risk significance model uses a risk rating minimum and risk rating maximum range to determine the risk significance value. For example, the risk rating will be an integer between 1 and 100, but you may only want five risk significance values. You would need to create five rows in the risk significance model using the minimum and maximum values:

Minimum	Maximum	Label
1	20	Low
21	40	Medium Low
41	60	Medium
61	80	Medium High
81	100	High

5

Control Management

Managing Controls Explained

Managing controls can consist of the following tasks:

- Viewing metrics on the Controls Overview Analytics tab: Control metrics can include control counts by class or trend, as well as other reports.
- Creating new controls: Create a new control when you require a policy, procedure, or other action to mitigate risks.
- Creating control test plans and instructions: These document steps to be followed in determining whether the control is effective and whether additional treatment is required.
- Creating control assessments: A control assessment is the review of policies and procedures that is performed to ensure that the controls are still effective and appropriate.
- Creating control issues (page 2-8): Create an issue to document any potential defects or deficiencies with the control itself or with specific assessment activities.

Creating New Controls: Critical Choices

When creating a control, consider the following:

- What type of control are you creating? There are three control types:
  - Preventive
  - Corrective
  - Detective
- What will the implementation method for the control be? You can select:
  - Manual: A manual control requires human intervention. For example, a manual control might be that an insurance policy must be reviewed for adequate coverage before annual renewal.
  - Automatic: An automated control does not require human intervention and is implemented or enforced by a system external to EGRCM. For example,

a control that prevents an individual user from both creating and approving an expenditure.

- How often should the control be run?
- What is the potential cost of the control?
- What assertions will this control evaluate? Assertions are statements of presumed facts about the status of a business process. For example, assertions can be made that financial assets exist and that financial transactions have occurred and been recorded during a period of time. Assertion types include:
  - Existence or occurrence
  - Completeness
  - Valuation or allocation
  - Rights and obligations
  - Presentation and disclosure
  - Accuracy
  - Cutoff
- Will this control be in scope for audit testing or assessments? Does this control require a test plan?

Creating Control Test Plans and Instructions

Test Plans Explained

After controls are identified to ensure that the response to the risk is properly executed, create control test plans and test instructions to test and validate the controls.

Creating Test Plans: Critical Choices

When creating test plans, you need to determine:

- What type of assessment is the test plan appropriate for? Choices are:
  - Operating assessment: Determines if the control operates effectively and as designed.
  - Certify: Determines if the information in the assessment is accurate and complete.
  - Design assessment: Determines if the control is designed effectively.
  - Audit test: Determines whether the control mitigates the risk and meets audit guidelines.
- What test instructions are required? Will the test instructions be manual or automated? Automated instructions describe steps that are performed in an external automated tool.

Creating Manual Test Instructions Explained

When creating manual test instructions, you need to determine what test instructions should be included. For example, if a control requires board of directors meetings to include monthly briefings on events and transactions that are not routine, manual test steps might include:

1. Record all meeting attendees.
2. Record and retain all meeting transcripts.

Creating Automatic Test Instructions Explained

Automatic test instructions are used when an external, automatic test will be run. When creating automatic test instructions, you are documenting that a test is performed by an external system by assigning the test instruction name and description. Optionally, you can add an attachment.

Editing Control Definitions Explained

When editing a control definition, you can:

- Change information about the control and its test plans.
- Add comments.

Any changes that you make to the definition are tracked through revision control.

See also "Creating New Controls: Critical Choices" (page 5-1) and "Creating New Base Objects: Critical Choices" (page 6-1).

Control Assessments Explained

An assessment is the systematic review of processes to ensure that controls are operating and designed effectively and appropriately. There are two methods of performing assessments:

- Create an ad hoc assessment (page8-3) from the Assessment tab of a control.
- Navigate to Assessment Management and:
    1. Create an assessment template (page 8-4).
    2. Create an assessment plan (page 8-5).
    3. Initiate the assessment (page 8-5).

For related information, see "Completing Assessments Explained" (page 8-6).

6

Managing Base Objects

Base Objects Explained

Base objects are general-purpose components that are used as defined in the module template. The Standard template includes six base objects, by default named Object A — Object F. During module definition, the base objects can be renamed as appropriate for the context in which they will be used. Renamed base objects appear in the Navigator.

Managing Base Objects Explained

Managing base objects can include the following tasks:

- Creating new components of the base object type. For example, in the Financial Governance module, you can create new process base objects.
- Creating action items.
- Managing revisions (page 2-6).
- Creating issues (page 2-8).
- Managing assessments.
- Viewing metrics on the Analytics tab of the overview page for a base object. Metrics include action item activity, overdue assessment activities, and other reports.

Creating New Base Objects: Critical Choices

When creating a new components from a base object, consider the following:

- Is this component in scope for audit testing and assessments? These indicators are used during assessment as selection criteria. When these criteria are used, only base objects that have been selected for the activity are brought into the assessment.
- If there is a perspective associated with the base object type, is the reference correct and complete? The Perspective region displays all perspectives that are

configured for the type of base object being created. You can view and manage the perspectives that are associated with the base object.

- Should any other objects be associated to the object you are creating? The objects that can be associated to a base object are determined during module setup. For example, in the Financial Governance module, you can associate a risk with the Process base object type.

When Would I Create an Issue for an Object?

Create an issue for an object when there might be a problem. For example, if you created a process for year-end closing, a possible issue might be that legal documents are required for year-end financial statements to be approved, but remain unsigned.

Base Object Assessments Explained

Perform an assessment to evaluate the validity and effectiveness of a base object. There are two methods of performing assessments:

- Create an ad hoc assessment (page 8-3) from the Assessment tab of a base object.
- Navigate to Assessment Management and:
  1. Create an assessment template (page 8-4).
  2. Create an assessment plan (page 8-5).
  3. Initiate the assessment (page 8-5).

For related information, see "Completing Assessments Explained" (page 8-6).

Action Items

Creating Action Items: Critical Choices

Create an action item for a base object when additional tasks are required. For example, if you have defined a process for year-end closing, you might require a task to verify that certain tax documents are included in the year-end reporting.

When creating a new action item, consider the following:

- What tasks need to be performed? Describe in detail how the action item must be accomplished. For example, say you suspect that some details of a recent acquisition were not recorded. The instructions might be: "Contact the finance department and obtain the details of last quarter's XY merger. Verify that they are recorded in the closing statements."
- When should this action item be accomplished? Two dates apply:
  - Due date: The date on which work on the action item must be completed.
  - Target completion date: The date by which the action item is expected to be completed. This date is entered by the person who performs the task. This field is available only when the action item is edited, not when it is created.

- What is the priority of this action item? The priority is reported in the metrics reports.
- What is the current progress of the action item? You can choose:
  - Assigned: The action item has been assigned, but work has not yet begun.
  - On Target: The assignee is working on the action item.
  - Delayed: Work on the action item will not be completed by the due date.
  - Blocked: No work can be done on the action item.
  - Completed: Work on the action item is finished, and it has been marked as complete.

What Is the Difference Between an Action Item and an Issue?

An action item is any task you might want to document. It is not necessarily a defect against the component. For example, if you have a year-end closing process component, the owner of the component might assign an action item to update a tax document before the year end. When the task is completed, the action item can be deleted.

However, if during the assessment of the year-end process component, the assessor notices that a tax document is out of date, then he would raise an issue against the component. Remediation for that issue would be to update the tax document.

What Is the Difference Between a Target Completion Date and a Due Date?

The due date is set when the action item is created; it is the date by which the task should be completed. The target completion date is set by the person who completes the task; it is the date on which that person expects to finish work. For example, if problems occur, the user can report his progress as Blocked and update the target completion date. Users who are responsible for completing action items cannot change the due date.

7

Issue Management

Issue Management Explained

Issue management can include the following tasks:

- Viewing metrics on the Issues Overview Analytics tab, including open issue by severity, issues awaiting remediation, and other reports.
- Creating issues.
- Creating remediation plans.

There are two ways to create issues:

- Via issue management as described in this section.
- In the context of the component definition, action, or assessment (see “Creating Issues: Critical Choices” on page 2-8).

Issues Explained

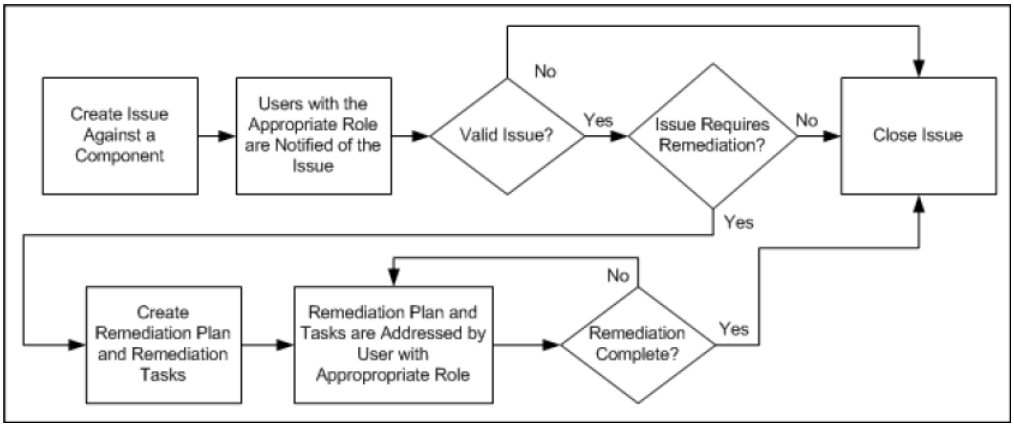
Issues are defects or deficiencies that are detected for an object or for an activity being performed against the object, such as an assessment. Issues can arise from within the context of the GRC business process. Each issue is associated with its related component, and reviewed in the context of that component.

Issue Life Cycle Explained

The life cycle of an issue is as follows:

1. The issue is created and assigned to users who have the appropriate privilege for the related object.
2. A worklist item to validate the issue is created and assigned to users who have the privilege to validate new issues. A user validates the issue and determines the disposition of the issue. The user can determine that the issue is valid, close the issue, or put it on hold.
3. If the issue is valid, a user with the appropriate privilege decides if a remediation plan is required to address the issue.

4. The remediation plan is defined and tasks are identified and assigned to users with the appropriate privileges.
5. A worklist entry to complete remediation tasks is created for users with the appropriate privilege.
6. A user responds to the worklist entry and completes the remediation task.
7. When all tasks are complete, the remediation plan is marked complete.
8. After the remediation plan is completed, the issue is closed.



Creating Issues: Critical Choices

Create a new issue to document reported defects or deficiencies against any component or its related activities, including risks, controls, base objects, or perspectives. When creating an issue, specify:

- The severity of the issue. The severity that you choose helps classify the issue, and can be used as a search and sorting aid.
- Any components related to the issue. When you create an issue from the Issue Management page, you must specify the component to which the issue is related.
- Any attachments (see page 2-6) that you want to associate with the issue.

Editing an Issue: Critical Choices

When editing an issue, consider the following:

- What action should be taken? When you put an issue on hold, the issue is considered valid, but resolution of the issue is deferred. Place an issue on hold when, for example, you require additional information to determine how to address the issue. You may also need to wait for a period of time before addressing an issue, for example the next month or quarter.

  Issue progress is tracked and metrics are provided for elapsed days between the time the issue was reported, dispositioned (that is, placed in Open or On Hold status), and closed.

  Issues are not automatically closed; users must close them manually. Once an issue is closed, it cannot be reopened.

- Does this issue require remediation? If so, create a remediation plan to address the issue and set the status to In Remediation. A remediation plan serves to document responses to an issue and to track the work required to resolve the issue.
- What is the financial impact of this issue? Quantify, in monetary terms, what the issue cost is to the organization. This is not used in any calculation or roll-up. It is measured in the currency specified for the related component.
- What is the chance that this issue will recur?
- Can this issue be closed? Close an issue when:
  - All remediation-plan tasks have been completed.
  - The remediation plan has been set to completed.

Creating Remediation Plans: Critical Choices

When creating a remediation plan, consider the following:

- What is the cost of the remediation?
- How much progress has been made on the remediation plan? Are the remediation tasks on schedule (On Target) or not (Delayed), or are you unable to make progress due to external forces (Blocked)? Progress for the remediation plan is derived from the status of the tasks. Progress for the issue remediation is derived from the status of the tasks for all remediation plans for the issue.
- What is the priority for completing this plan?
- Have any of the associated remediation tasks been completed, and can they be marked as such?

What Is the Difference Between a Target Completion Date and a Due Date?

The due date is set when the task is created; it is the date by which the activity should be completed. The target completion date is set by the user who performs the task; it is the date on which that person expects to finish work. This serves to report the progress of the activity. For example, if problems occur, an assignee can report her progress as Blocked and update the target completion date.

Creating a Remediation Task: Critical Choices

When creating a new remediation task, consider the following:

- What is the priority for completing this task? The priority is taken into account for issue reporting.
- How much progress has been made on the remediation task? The user who performs the task updates it with the current progress, specifying if the task is on schedule (On Target) or not (Delayed), or if she is unable to make progress due to external forces (Blocked).
- What is the status of the task? Status can be specified either as the task is created or when it is edited by the user who works on completing it. Possible statuses are In Progress (Active) and Complete.

- What specific task needs to be performed? For example, say you created an issue during an operational assessment of a control — there are no instructions for the test plan, and that caused the assessment to fail. The remediation plan is to correct the control test plan definition, and remediation tasks might be:

  1. Determine the steps needed to test this control.
  2. Update the test plan instructions.

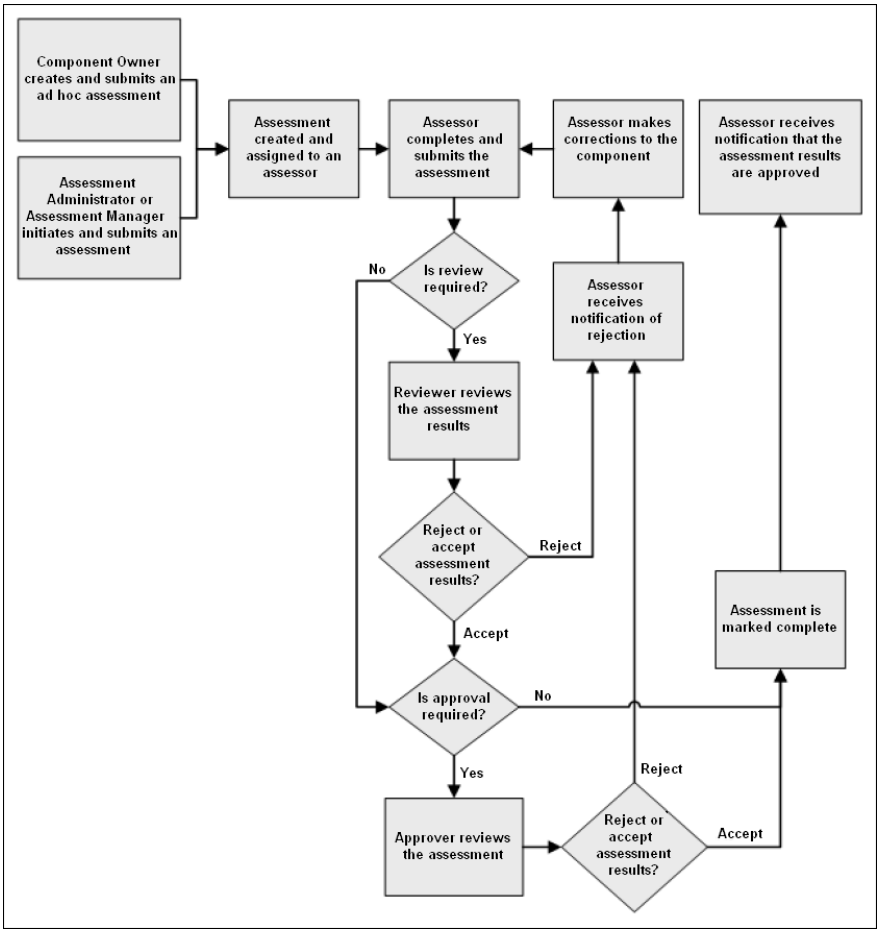
8

Managing Assessments

Assessments Explained

Components such as risks and controls require periodic review of how they are defined and implemented to ensure that the appropriate levels of documentation and control are in place. This process is called an assessment, where an evaluation is made about the validity and effectiveness of controls, risks, perspectives, and base object components.

The assessment process flow is:



1. The assessment is initiated. Whether the assessment is ad hoc or initiated via the Assessment Management page, the process after initiation is the same for all objects except perspectives. Refer to "Perspective Assessments Explained" (page 3-3) for details of the perspective assessment flow.
2. The assessor completes and then submits the assessment.

   Note: The assessment review and approval processes are performed only if there are users who have the appropriate roles to perform those tasks. If no users have these roles, the review and approval processes are skipped and the assessment goes into Complete status after the assessment is submitted.
3. A reviewer either accepts, rejects, or requests information regarding the assessment. If the reviewer rejects the assessment result, the assessment result state is set to Reject and a notification is sent to the assessor. The review approval process is terminated and all outstanding worklist entries are rescinded. If the reviewer accepts the assessment, a worklist entry is created for the assessment approver.

   Note: There can be multiple reviewers. The assessment will not proceed to the approver until the assessment is no longer in the In Review status.
4. The approver can request additional information, accept the assessment, or reject it. If the approver rejects the assessment result, the assessment result state is set to Reject and notification is sent to the assessor. If the approver accepts the assessment, it is marked as complete and the assessor receives notification that the assessment has been approved.

   Note: There can be multiple approvers. The assessment will not be placed in Complete status until the assessment is no longer in the Awaiting Approval status.

Assessment Activities Described

You can perform the following assessment activities:

- For risks:
  - Assess risk: Determine if controls are operating effectively to mitigate a risk. Answer the question, "Is the risk appropriately documented, is the analysis current, is the evaluation accurate, and are the treatments active?"
  - Audit risk: Assess whether the risk meets audit guidelines.
  - Certification: Answer the question, "Is the information in this assessment accurate and complete to the best of my knowledge?" All resources that have an active role in the accuracy of the assessment are typically required to answer this certification question and to provide supportive comments.
- For controls:
  - Audit test: Determine whether the control meets audit guidelines.
  - Operational assessment: Determine if the control operates effectively and as designed.
  - Certification: Answer the question, "Is the information in this assessment accurate and complete to the best of my knowledge?" All resources that have an active role in the accuracy of the assessment are typically required to answer this certification question and to provide supportive comments.

  - Design review: Determine if the control is designed effectively and meets its objectives.
- For base objects:
  - Operational assessment: Determine if the base object operates effectively and as designed.
  - Certification: Answer the question, "Is the information in this assessment accurate and complete to the best of my knowledge?" All resources that have an active role in the accuracy of the assessment are typically required to answer this certification question and to provide supportive comments.
  - Design review: Determine if the base object is designed effectively and meets its objectives.
  - Audit test: Determine whether the base object meets audit guidelines.
  - Documentation update: Determine if the base object has required documentation.
- For perspectives, certification: Answer the question, "Is the information in this assessment accurate and complete to the best of my knowledge?" All resources that have an active role in the accuracy of the assessment are typically required to answer this certification question and to provide supportive comments.

Methods of Initiating Assessments Described

There are two methods of initiating assessments:

- Create an ad hoc assessment from the Manage page for an object.
- Initiate an assessment from the Assessment Management page.

You can create an ad hoc assessment quickly, but the assessment can be used only once. If you create an assessment from the Assessment Management page, you must create a template and a plan, and then initiate the assessment. The advantage of this is you can reuse the plans and templates as often as needed.

Ad Hoc Assessments Explained

You can create ad hoc assessments for risks, controls, base object components, and perspectives.

Create ad hoc assessments for risks, controls, and base object components from the manage object page. Use one of the following:

- From the Assessments tab, click the New icon.
- Choose Create Assessment from the Action menu.

To create ad hoc assessments for perspectives, do one of the following:

- From the Manage Perspective page, choose Create Assessment from the Action menu.
- Select the hierarchy on the Manage Perspective Hierarchies page and click the Create Assessment button.

Assessment Management Explained

Assessment management tasks include:

- Creating assessment templates.
- Creating assessment plans.
- Performing management tasks on assessments assigned to you, including initiating assessments and completing assessments.
- Reviewing assessment results.

From the Manage Assessments page, you can:

- Click on an assessment name to invoke the Manage Assessment Details page, on which you can view the component and activity details for the assessment.
- Close an assessment. An assessment initiated from Assessment Management can be closed only by the person who initiated it. In most cases, the assessment is closed either when the due date is reached or when all individual assessments within the initiated assessment batch are completed. Assessments are displayed as long as the assessment plan is active, even if the assessment is complete.
- Modify the date by which the assessment must be completed.

Managing Assessments

Click the My Assessments task link to view the assessments assigned to you. From the My Assessments page, you can:

- Complete an assessment.
- View prior approvals for the assessment and, if necessary, withdraw approval for an assessment you own.
- Create an issue for the assessment (page 7-2).

Creating Assessment Templates: Critical Choices

An assessment template is a collection of assessment activities. Assessment templates also display user-defined component relationships and their related assessment activities. When creating an assessment template, consider:

- Which module or perspective will this template be used to assess?
- What is the primary object to be assessed? If you select a perspective, you will be able to select from a list of perspective hierarchies. If you select a module, you will be able to select from a list of primary components.
- What type of assessment will you perform? For example, you might need to prepare financial year end or financial SOD assessments.
- What activities (page 8-2) will be performed during this assessment? Depending on the component you have added, you can choose activities such as audit test, operating assessment, design assessment, or certify.

Assessment Plans Explained

Creating Assessment Plans: Critical Choices

Create an assessment plan to describe criteria for the assessment activities that are associated with an assessment template. When creating an assessment plan, consider the following:

- With which component will this plan be associated?
- Which assessment template will this plan use? The options that you can choose from depend on the component you choose. You can select only active templates.
- Does this plan require a survey template to be attached? A survey template can be included on any assessment activity for components.
- What selection criteria do you want to specify? The selection criteria determine the specific controls, risks, and other components that will be assessed.
- What perspective selection criteria do you want to specify? Entering a perspective in the selection criteria provides an additional filter for the data. For example, if you choose the Organization perspective and select one of the child nodes within it, the assessment will include only the assessment components that are within the hierarchy of that perspective node.

What Is the Difference Between an Assessment Template and an Assessment Plan?

An assessment template specifies the assessment activities. An assessment plan specifies which components will be used in the assessment. The assessment plan references the assessment template, and many assessment plans can reference a single assessment template. When you initiate an assessment, you indicate which assessment plan to use.

Initiating Assessments Explained

When you initiate an assessment, you select an active assessment plan. The assessment template drives the assessment activities. When you initiate, you can override the selection criteria, but you cannot change the assessment activities. If a survey template is associated with assessment activity, a survey is initiated. You can schedule an assessment's start date and specify a due date during the creation of the assessment plan. You can also review and override individual objects from the assessment plan selection criteria.

Initiating an Assessment: Critical Choices

When initiating an assessment, consider the following:

- Which assessment plan will you use? The plan contains the criteria for the assessment activities associated with the assessment template.
- When must the assessment be started and completed? The assessment will not appear on the assessor's worklist until the start date.

- What selection criteria are needed? You can refine the selection criteria from what was specified in the assessment plan. Additional criteria for controls (stratification) are available when the assessment includes controls. When the primary component is not control, but controls are within the assessment, the system checks the control stratification on the risk; if the condition is met on any risk, the control is included in the assessment. See "Editing Related Controls: Critical Choices" on page 4-3.
- What components will be assessed? The components that you can choose from are based on the information model's primary component and are filtered depending on the application mode. To see available components, click the Generate button.

Completing Assessments Explained

You can use any of the following methods to complete any risk, control, or base object component assessment that is assigned to you:

- Select the assessment from your worklist and click the Edit icon.
- From the object's Assessments page, select the assessment, then click the Complete or Review/Approve button, depending on your role and the status of the assessment.
- From the Assessment Management page, click the Complete Assessments link.

  Note: The process of assessing and certifying a perspective is different from that of all other objects. To complete an assessment on a perspective, refer to "Perspective Certification Process Explained" on page 3-3.

Depending on the object you are assessing, you are presented with some or all of the following screens as you complete the assessment:

- The introduction screen presents an overview of the object being assessed. This includes details of the assessment, the component being assessed, and any related components, perspectives, or issues. If your GRC Administrator has created any user-defined attributes for the object being assessed, you will see the UDA information in an Additional Details region.
- The Prior Results screen displays results from prior assessments. The state of assessments can be:
  - New: The assessment has been initiated but not started.
  - In Review: The assessment is being reviewed by a user who has assessment review privileges.
  - Awaiting Approval: The assessment is being reviewed by a user who has assessment approver privileges.
  - Rejected: The assessment has been rejected at the review or approval stage.
  - Complete: The assessment has been completed, reviewed, and approved. An assessment is considered valid only if it is in Complete status.

    Note: Before an assessment is submitted, it is in New status. After it is submitted, it stays in Active status until it is Closed.

- If you are assessing a control that has a test plan attached to it, you can complete the test plan on the Enter Results screen.
- If a survey is attached to the assessment plan, you can complete it on the Survey screen.
- On the Complete Assessment page, you can:
  - Enter the results of the assessment. Refer to the assessment process flow (page 8-1) for details of what happens after an assessment is approved.
  - Create an issue (page 7-2) if you fail the assessment and wish to track the problem.
  - If you have the appropriate privileges for the object being assessed, you can specify an attachment (page 2-6) to include additional information with the assessment results.

Reviewing and Approving Assessments Explained

If you are notified that there are assessment results to review or approve, do one of the following:

- From your worklist, select the assessment results and click the Edit icon.
- From the Assessment tab on the object, select the assessment and click the Review/Approve button.

Review the assessment results and either pass or fail the assessment as appropriate. If you do not agree with the assessment results, you can fail the assessment, which returns it to the original assessor's worklist. Refer to the assessment process flow on page 8-1 for details of the process flow.

Note: The process of assessing and certifying a perspective is different from that of all other objects. To certify a perspective, refer to "Perspective Certification Process Explained" on page 3-3.

What Do the Assessment Result Options Mean?

The following results options are seeded in the application. Your GRC Administrator can modify the names of the result options via the Setup and Administration Manage Assessment Results page, so the results options that you see may differ from those described here.

For design, operating, and audit test assessments:

- Pass: The object is operating properly to mitigate the risks.
- Pass with exception: The object is operating properly to mitigate risks, with noted exception.
- No opinion: You have reviewed the object but do not have a definitive judgment of whether it should pass or fail.
- Failed: The object does not operate properly to mitigate risk.

For certify assessments:

- I agree with this statement: The information in the assessment is accurate.
- I agree with this statement with the noted exception: The information in the assessment is accurate with noted exceptions.
- I do not agree with this statement: The information in the assessment is not accurate.
- No opinion: You either cannot or choose not to make a statement regarding the assessment.

For documentation update assessments:

- Complete: The required documentation is complete.
- No action: The documentation is sufficient and no additional action is required.

9

Managing Surveys

Managing Surveys Explained

Surveys are used to assist in evidence gathering for assessments and other testing. You can also create general surveys unrelated to assessments or testing. These may include any type of question, for example questions concerning customer satisfaction. Managing surveys involves the following tasks:

- Managing survey questions.
- Managing survey choice sets.
- Managing survey templates.
- Creating (initiating) and editing surveys.
- Viewing responses to surveys by selecting View Responses from the Manage Survey page.
- Managing survey versions and revisions (page 2-6).
- Deleting surveys.

Surveys are created from survey templates. Surveys include a set of users (called responders) who must respond to the survey, the time frame during which users can respond, and instructions on how to respond. If a survey is generated from an assessment, it cannot be managed or edited outside of the assessment.

Managing Survey Questions

Creating Questions: Critical Choices

When creating survey questions, consider:

- What type of question will this be? You can choose 302 Organization Certification or General, or any other question type that your survey manager has created.
- What will the format of the question be? The format type for the question identifies how the responses to the question are presented. Options are:
  - Single response: Radio buttons present multiple options; a respondent can select only one of them.

  - Single response with other: Radio buttons present multiple options; a respondent can select only one of them. One option is *Other*, which includes a text field in which the respondent can enter a value.
  - Single response drop down list: A list of values presents multiple options; a respondent can select only one of them.
  - Multiple choice list box: A scrolling list box presents multiple options; a respondent can select any number of them.
  - Check all that apply: Check boxes present multiple options; a respondent can select any number of them.
  - Check all that apply with other: Check boxes present multiple options; a respondent can select any number of them. One option is *Other*, which includes a text field in which the respondent can enter a value.
  - Rating on scale: Radio buttons present a range of values; a respondent can select only one of them. For example, a question may be "How often do you use this tool?" Responses may range from *Always* to *Never*.
  - Numeric allocation: A respondent enters a number for each of several options, quantifying each in comparison to the others. For example, a question might be, "What percentage of your monthly minutes to you allot for the following features on your cell phone?" Options might be *Email*, *Texting*, *Voice*, and *GPS*; the respondent would provide a number for each, and the numbers would add to 100 percent.
  - Open text: A text box enables respondents to enter free-form text.
- What choice set contains the appropriate answers to the question? You can specify an existing choice set or create a new one. If you choose an existing choice set, you can edit it to suit your needs. For example, you can select a choice set that contains the values *Yes* and *No*, and create your own value, *Maybe*. Or you could select the choice set *High*, *Medium*, *Low*, and delete *Medium*. You can save any new combination of answers as another choice set for use in the future.

Managing Survey Choice Sets

A choice set is a collection of answers to be used as a short cut for completing questions. For example, a choice set could contain the answers *I agree* and *I disagree*, or *High*, *Medium*, and *Low*, or *Yes* and *No*. The answers could be appropriate for a large number of questions. Using choice sets provides reusability of answers as well as consistent recognition to the same answer across questions. Managing choice sets can consist of the following tasks:

- Creating new choice sets: Either add existing answers to a new choice set, or click the Create New Choice button to create a new answer, then add that new answer to your new choice set.
- Editing existing choice sets.
- Duplicating choice sets: If an existing choice set has answers similar to those you require, you can duplicate it and then edit it to add new answers or to delete answers you do not need.

Managing Survey Templates

Creating a Survey Template: Critical Choices

Survey templates are used to help form surveys. When creating a survey template, consider:

- What type of survey will this template be used for? Options include Financial Compliance, 302 Certification, General, or any other type that your survey manager has created.
- Do respondents require any special instructions for filling out the survey?
- Will the template have to be translated and, if so, into what languages? Options include the languages that your installation is using. This field is informational only. Translation is not automated; it is a manual task performed by translators.
- What questions are part of the survey? You can create new questions or reuse existing questions.
- How do you want the survey displayed? You can format the survey by inserting page breaks at any point.
- Is the survey template as you expect? Use the Preview button to verify that the format and layout of the questions are as you intend.

What Happens When I Delete a Survey Template?

You can delete a survey template only when it is in a New state. Once the template is Active, it cannot be deleted. When a survey template is deleted, the template is no longer available. However, the questions associated with it are not deleted, and all historical data remains.

Survey templates can be made Inactive. However, you cannot inactivate a survey template if surveys use that template and are open to collect responses. Once a survey template is inactivated, all users associated with the survey receive a notification displayed in the pending activities section of the dashboard or overview pages.

Creating and Editing Surveys Explained

You can create general surveys that are not related to an assessment. To create a survey, select the New icon from the Manage Survey screen, then select the template on which you wish to base the survey. When initiating the survey, you must decide:

- When should this survey be completed? An end date is required, but you can edit the date and extend the survey period if needed.
- Is this survey associated with a type of object? This is a required field.
- Is this survey associated with a specific object? This is a required field.
- Which users need to respond to this survey? You can choose individual users or you can select from an existing list. You can also save the respondents list for future use.

Once you have submitted your survey, the only edits you can make to it are the end date and respondent list.

Completing Surveys Explained

If you are designated as a survey respondent, the survey appears in your worklist. To complete the survey, select the survey and click the Edit icon. Once you have submitted the survey, the originator can view your responses via the Survey Management page.

10

Reporting

Reports Explained

EGRCM includes reports that address business questions across various entities such as risks, control, and issues, as well as security and administration reports. Some reports are specifically designed for the Financial Governance module. The reports provide flexibility — you can choose from a wide range of criteria to specify information to include in them. Access to reports is based on the roles assigned to users.

Each report is designed with a different business requirement and criteria, and you can specify exactly what you want to appear in your report. The general procedure to run a report is:

1. From the Navigator, choose Report Management.
2. Select the type of report you want to run. Options include:
   - GRCM Assessment Tools Reports
   - GRCM Issue Management Reports
   - GRCM Control Management Reports
   - GRCM Risk Management Reports
   - GRCM Security Reports
   - GRCM Admin Reports
   - GRCM Action Reports
3. Select the report you want to run. Refer to “Delivered Reports” (page 10-2) for details on reports.
4. From the Action menu, choose either to run a report immediately or to schedule a report for a future time.
5. Select values that filter the content of your report, so that it includes only information you want to see. Filtering criteria vary from one report to the next.
6. If you chose to run a report immediately, select the Generate Report button. If you chose to schedule a report, click the Schedule Information button. In a Schedule Parameter form, enter values that set a name for the schedule, the date and time at which it should start, the regularity with which the report should

run, and the date and time (if any) on which the schedule should expire. Then click the Schedule button.

Delivered Reports

The following reports are available:

- GRCM Assessment Tools Reports
  - Control Assessment Details Report: Displays all information about a specified control.
  - Control Assessment Extract: An Excel report that lists controls and their related assessment activities.
  - Control Assessment Report
- GRCM Issue Management Reports
  - Issue Details Report
  - Issue Listing Extract: An Excel report that lists issues and their related objects.
- GRCM Control Management Reports
  - Control Details Report
- GRCM Risk Management Reports
  - Risk Control Matrix
  - Risk Control Matrix Extract: An Excel report that lists risks, controls, and related information (perspectives, UDAs, etc.).
- GRCM Security Reports
  - Inaccessible Records Report: Displays records no user can access. No user has the correct functional or data privileges to access the record.
  - Record Assignment Report: Displays job roles, users who have specific job roles, and what access they have to objects.
  - Role Assignment Report: Displays the roles that each user has within EGRCM. You can enter a job role, and the report displays users assigned that role.
  - Unassigned Data Privileges Report: Displays perspective values with related objects, for which no job role has the correct privileges. This report can reveal potential holes within your data security.
- GRCM Admin Reports
  - Change History Report: Displays the change history for selected objects.
  - Pending Activity Report: Displays the outstanding worklist items by user.
  - Worklist Items Requiring Reassignment
- GRCM Action Reports
  - Related Objects Report

11

Administration Tasks

Managing Application Configurations

Use the Manage Application Configurations page to set parameters required for EGRCM to connect to its database and to set other properties. You can set up EGRCM to recognize users created externally in a database that uses LDAP technology to share user information.

Properties Tab

Use the Properties tab to set values required for EGRCM to connect to its database, to establish a set of languages EGRCM uses to display information to its users, and to select performance options. When configuring properties, you can specify:

- Installation Configuration
  - User Name: Supply the user name for the GRC database.
  - Password: Supply the password for the GRC database.
  - Confirm Password: Re-enter the password for the GRC database.
  - Port Number: Supply the port number at which the GRC database server communicates with other applications.
  - Service Identifier: Supply the service identifier (SID) for the GRC database server.
  - Server Name: Supply the fully qualified domain name of the database server.
  - Report Repository Path: Supply the full path to your Report Repository. This is a directory, established during installation, that stores report history.
  - Log Threshold: Select a value that sets the level of detail in log-file entries. From least to greatest detail, valid entries are *error*, *warn*, *info*, and *debug*.
- Language Preferences: Choose languages available to EGRCM users — select their check boxes. (Or, clear check boxes to make languages unavailable.) Once selected here, languages are available for selection by administrators as they create user accounts and individual users as they configure their user preferences.

- Performance Configuration
  - Externalize Report Engine: Select the check box to enable the reporting engine to run in its own java process, so that the generation of very large reports does not affect the performance of other functionality. However, select the check box only if you have installed EGRCM on hardware that is identified as "certified" in the *Governance, Risk and Compliance Applications Compatibility Matrix*; clear the check box if you use hardware identified as "supported."
  - Optimize Appliance-Based Operation: Select the check box to optimize performance if the EGRCM application and GRC schema reside on the same machine. Do not select this check box if the EGRCM application and schema do not reside on the same machine. When you select this check box, an ORACLE_HOME Path field appears. In it, enter the full, absolute path to your Oracle Home — the directory in which you have installed the Oracle database that houses the GRC schema.

Worklist Tab

If you have installed EGRCM with SOA, you can configure the following worklist settings:

- Worklist Server User Name: Enter the ID, created during installation, for the SOA administrative user. Typically this value is *soaadmin*.
- Worklist Server Password: Enter the password created during installation for the soaadmin user.
- Worklist Server Confirm Password: Re-enter the Worklist Server Password.
- Worklist Server URL: http://*host*:*port*, in which *host* is the IP address of your SOA server, and *port* is its port number. (The SOA server is either a managed server in a GRC domain created during EGRCM installation, or a SOA server used by EGRCM even though it had initially been set up for other purposes. See the *Governance, Risk and Compliance Installation Guide*.)
- Worklist Server Protocol: Select the communications protocol — either SOAP or RMI — used by the GRC application to send and receive SOA requests.

Security Tab

You can set the following security options:

- Maximum Login Attempts: Enter the number of times a user may enter an incorrect user name or password during login before being locked out of EGRCM. (Administrators can use the Manage Users page to unlock user accounts.)
- Elapsed Days Before Password Expires: Enter the number of days for which EGRCM login passwords remain valid. When each user's password expires, the user is prompted to create a new one during login.
- Use Basic Authentication for Web Service: Select this checkbox as one step in integrating EGRCM with an application whose database shares its user information through LDAP technology. However, there are limitations that could materially affect data and functionality. Therefore, you should configure LDAP inte-

gration in general, and select the Use Basic Authentication for Web Service field in particular, only with the assistance of Oracle Consulting Services or another organization experienced in this type of integration for EGRCM. (Also, see "User Integration Tab," below.)

Analytics Tab

EGRCM can supply data to Governance, Risk and Compliance Intelligence (GRCI), which supplies dashboard and reporting services. To do so, EGRCM places data in a schema distinct from its principal one, known as the "Data Analytics" (DA) schema.

For all of this to occur, you need to create the DA schema, then complete fields in all three of the sections on this Analytics tab: Data Analytics Configuration, Analysis, and GRC Intelligence Configuration. Typically, these fields are completed during installation and their values should not be changed subsequently. See the *Governance, Risk and Compliance Installation Guide* for version 8.6.4.

You can set a schedule on which the DA schema is refreshed — on which the DA schema reads data from the GRC schema. To do so, click the Schedule Data Analytics Update button and complete scheduling fields.

User Integration Tab

EGRCM can be integrated with an application whose database shares its user information through LDAP technology. However, there are limitations that could materially affect existing data and functionality. Therefore, this should be done only in conjunction with professionals experienced in this type of integration for EGRCM. Contact Oracle Consulting Services or another experienced organization for assistance. (Also, see the discussion of the User Basic Authentication for Web Service field in "Security Tab," page 11-2.)

- Single Sign On: Select the Enable Single Sign On check box to make use of Single Sign On, which establishes a single set of log-on credentials for each user in varying applications. (Or, clear the check box to turn off Single Sign On.)
- External LDAP User Repository
  - Enable Integration: Select the check box to permit user integration to occur.
  - User Name: Supply the user name for the LDAP database schema.
  - Password: Supply the password for the LDAP database schema.
  - Confirm Password: Re-enter the password for the LDAP database schema.
  - Port Number: Supply the port number at which the LDAP database server communicates with other applications.
  - Server Name: Enter the host name of the LDAP database server.
  - Bind DN Suffix: Supply the common suffix added to each user ID to form the LDAP Bind DN. (Each user must have a UID attribute.)
  - Users Organizational Unit: Supply the "container" in the LDAP hierarchy that holds user records.

Notification Tab

Establish a connection with your SMTP server for notifications and set a notification schedule.

- Notifications Server
  - User Name: The user name with which one would log on to the SMTP server. This value is required only if access to the SMTP server requires authentication.
  - Password: The password with which one would log on to the SMTP server. This value is required only if access to the SMTP server requires authentication.
  - Confirm Password: The SMTP server password entered in the Password field. This value is required only if access to the SMTP server requires authentication.
  - Port Number: The port number at which the SMTP server communicates with other applications.
  - Server Name: The host name for the SMTP server your company uses for sending email.
  - Sender Email Address: An address that appears in the "From" line of email messages generated by the Notification function.
  - Application URL: The URL for your instance of EGRCM. This takes the form http://*host*:*port*/grc, in which *host* is the fully qualified domain name of your GRC server, and *port* is the port number selected for it when its web application server was configured during installation.
  - Enable SSL Authentication: Select this check box if access to your SMTP server requires authentication; clear the check box if it does not. If authentication is required, the User Name, Password, and Confirm Password fields must also be populated (see above).
  - Enable Notification: Select this check box to activate the sending of notifications, or clear it to inactivate the sending of notifications.
- Notification Schedule
  - Start Date: Enter a date (in the format *mm/dd/yyyy*) on which the sending of notifications should begin. Alternatively, click on the icon to right of the field; a pop-up calendar appears. Click left- or right-pointing arrows to select earlier or later months (and years), and then click on a date in a selected month.
  - Start Time: Enter a time (in the format *hh:mm*) at which the sending of notifications should begin on your start date.
  - Hourly Interval: Enter a number that expresses the period (in hours) between which notifications are sent.
  - Run Now button: Click to send notifications once, immediately. To use this option, you need not enter values in the scheduling fields. If a schedule has been set, however, it will continue to be honored; the use of the Run Now button does not affect it.
- Notification Content: Select the Include All Worklist Entries check box to cause email content to include a list of EGRCM worklist items appropriate for the recipient.

Managing Installation Options

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

- What is the local currency for this installation? Because only one currency is supported throughout the installation, the currency that you select is used wherever monetary amounts are entered.
- What likelihood and impact models do you wish to set as defaults?

Managing Lookup Tables

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

When managing lookup tables, consider the following:

- Which lookup type do you need to update? This is the name of the lookup table. You can add new lookup codes to the following lookup types:
  - GRC_ASSESSMENT_TYPE
  - GRC_CONTROL_AUDIT
  - GRC_CONTROL_FREQUENCY
  - GRCM_CONTROL_TYPE
  - GRC_CTRL_ASSERTIONS
  - GRC_ENFORCEMENT_TYPE
  - GRC_ISSUE_LIKELIHOOD
  - GRC_ISSUE_REASON
  - GRC_ISSUE_SEVERITY
  - GRCM_ISSUE_TYPE
  - GRCM_PERSPECTIVE_TYPE
  - GRCM_PROCESS_TYPE
  - GRAM_REMEDIATION_PLAN_TYPE
  - GRC_REMED_PLAN_PRIORITY
  - GRC_REMED_TASK_PRIORITY
  - GRCM_RISK_TYPE
  - GRC_SURVEY_QUESTION_TYPE
  - GRC_SURVEY_SURVEY_TYPE

- What will be the code for the lookup value? This is the identifier for the lookup value. For example, if a lookup is to be a range, the codes in the lookup might be integers from 1 to 5.
- What is the meaning for the lookup code? This is the descriptive term used for the code and is the value that the user selects from a list of values. For example, the meaning of the code 1, on a scale of 1 to 5, might be *Lowest*.
- What is the description for this lookup value?
- Used for User Defined Attribute checkbox: Select for each value that is to be used with a UDA.

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

- Type: GRC_VALUESET_RISK_LEVEL
- Code: 1
- Meaning: Low
- Description: Low risk level
- Used for User Defined Attribute checkbox: Selected

Managing Content Types

When you add an attachment to an object, you must specify a content type. You can create new content types as needed. When creating a new content type, specify:

- Content Code: This is an internal identifier and must be unique.
- Description: This appears on the menu where users select the attachment content type.

Managing the URL Repository

Use the URL Repository to manage links that are available when you create a UDA with a link data type. When you add a new URL to the repository, you can specify:

- Name: This is a required field. The name of the link can have up to 150 characters.
- Description: Use this optional field to describe the URL. The description can have up to 255 characters.
- URL Address: This is a required field that can contain up to 1,000 characters.

Managing Assessment Results Explained

You can edit the name of the response that is displayed to users when they are performing an assessment. You cannot create new responses, you can only edit existing delivered responses. For example, you might want to change the existing response, “Requires Additional Analysis,” to something more specific to your organization, such as, “Requires Analysis from District Manager.”

12

Managing Security

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

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

To define access to data, EGRCM uses these components:

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

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

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

Managing Duty Roles

Many duty roles are delivered for use in the Financial Governance module. Create a new duty role when there is no delivered duty role that suits your needs:

1. From the Navigator, choose Setup and Administration.

2. In the Security tasks, choose Manage Roles.
3. From the Actions menu, choose Create Duty Role.
4. Enter a name and description for the new role.
5. Enter a status — Active or Inactive — for the new duty role.
6. Click Actions > Select Privileges, or select the Add button (a green plus sign), to choose the privileges for the duty role. You can query by example (page 2-3) to limit the list of privileges to those that meet certain criteria.
7. When you have selected all the privileges you want, click the Save button or the Save and Close button.

You can also create new duty roles by copying existing duty roles (page 2-6).

Managing Data Roles

Data roles control access to data in the application. Each defines filters, which specify sets of data either to be made available to, or excluded from, the role.

Each filter expresses a relationship between an attribute and a value. It might, for example state that module (the attribute) equals Financial Governance (the value), or it might identify a particular perspective (the attribute) then specify a node within that perspective (the value). Depending on further configuration, the role would include or exclude data belonging to the item that satisfies the defined relationship (for example, data belonging to the specified node in a perspective).

The only delivered data role provides access to the Financial Governance module. You can create additional data roles. First, open the Create Data Role page and set up the role itself:

1. From the Navigator, choose Setup and Administration.
2. In the Security tasks, choose Manage Roles.
3. From the Actions menu, choose Create Data Role.
4. Enter a name and description for the new role.
5. Enter a status — Active or Inactive — for the new data role.

Next, create one or more filters for the role:

1. In the Filters list, click the Add button (a green plus sign). A new row appears in the list.
2. In the Filter Name field, enter a name for the filter.
3. In the Object field, select Data Attributes or Perspectives. Your choice determines the selections you can make in the Attribute field.
4. If you selected Data Attributes in the Object field, select one of these values in the Attribute field: DataRole, Module, State, or StateAction. You would select Module, for example, to specify data associated with a module you have created, or you could select DataRole to specify data associated with an already-existing data role.

If you selected Perspectives in the Object field, select a configured perspective hierarchy in the Attribute field. Your filter (with some further refinement) would select data associated with the perspective you select.

5. If you selected Data Attributes in the Object field, select either Equals or Not Equals in the Condition field. If you selected Perspectives in the Object field, choose Equals, Not Equals, or Includes Children in the Condition field.

6. In the Values field, click on a button that looks like a magnifying glass. A pop-up window opens; in it, select a value that completes the relationship definition already begun in the Attribute and Condition fields.

   For example, if your attribute is Module and your condition is Not Equals, your value will be the name of a specific module; this would designate data belonging to all modules other than the one you've named.

   Or, if your attribute is a perspective named Activity, and your condition is Equals, your value may be the name of a node within the Active hierarchy (for example, Certification); this would designate data associated with that node. Or, if your condition is Includes Children, the filter would designate data associated with the node you select and all of its child nodes.

7. In the Include/Exclude list box, select Include to allow access to the data you've defined, or Exclude to prevent access to the data you've defined.

8. When one filter is complete, optionally repeat this process to create additional filters. You may create as many filters as you need to define a specific set of data. (Filters have an AND relationship; the role captures only data that satisfies all the filters you define.)

When you're satisfied with your filter definitions, click on the Save or Save and Close button.

You can also create new data roles by copying existing data roles (page 2-6).

Managing Job Roles

Many job roles are delivered for use in the Financial Governance module. Create a new job role when there is no delivered job role that suits your needs:

1. From the Navigator, choose Setup and Administration.
2. In the Security tasks, choose Manage Roles.
3. From the Actions menu, choose Create Job Role.
4. Enter a name and description for the new role.
5. Enter a status — Active or Inactive — for the new job role.
6. Click Actions > Select Roles, or select the Add button (a green plus sign). An Add Role pop-up window opens; in it, select a combination of duty, data, and existing job roles that would enable users assigned this role to do their jobs. You can query by example (page 2-3) to limit the list of roles.
7. Click on the Save or Save and Close button.

You can also create new job roles by copying existing job roles (page 2-6).

Managing Users

You can create new users, edit existing users, copy users, or import users from LDAP.

Creating New Users

To create a new user:

1. From the Navigator, choose Setup and Administration.
2. In the Security tasks list, choose Manage Users.
3. From the Actions menu, select Create User.
4. Enter values in the Details section of the Create User page.
    - In the Username field, type a name by which the user identifies herself as she logs on. A username consists of alphanumeric characters, may be any length, and is not case-sensitive.
    - In the Last Name, First Name, and Middle Name fields, enter the user's surname, given name, and middle name. (The middle name is optional.)
    - In the Email Address 1 field, supply an email address for the user. EGRCM uses this address to send notifications to the user.
    - Optionally, provide tracking information — a second email address, office and mobile phone numbers, physical address, and the user's position and organization — in the appropriate fields.
    - In the Status field, select a status for the user — typically Active. You would select Inactive if a user is no longer eligible to use EGRCM (for example, if the user resigns from your company). You can also select Locked, although typically this status is set automatically by EGRCM if the user fails to log on properly after a number of attempts specified in the Security tab of the Manage Application Configurations page.
    - In the Language field, select a language in which EGRCM will display information when the user logs on. An administrator uses the Properties tab of the Manage Application Configurations page to select languages in which EGRCM can display information. This field enables you to choose one language from among that administrator's selection.

      The user can override this setting by selecting a new language while configuring preferences (page 2-5).
    - In the Password field, type a password with which the user validates her user name as she logs on. Retype the password in the Confirm Password field. A password is case-sensitive and must consist of at least eight characters, taken from each of four character sets: uppercase letters, lowercase letters, numbers, and special characters, which comprise !@#$%&*. Moreover, the password is invalid if it matches or contains the user name.

      The user's password expires periodically. (The period is set in the Security tab of the Manage Application Configurations page.) When the user logs on for the first time, or when the password expires, the user is prompted to

create a new one as she logs on. The new password must not match any of the previous three passwords.

5. In the Selected Roles area, assign roles to the user. Select Actions > Assign Roles, or click the Add button (a green plus sign). An Add Role pop-up window appears. In it, select any number of roles you want to assign. (Use the Shift or Ctrl key to select continuous or discontinuous sets of roles.) Then click the OK button; the pop-up window closes, and the chosen roles appear in the Select Roles area.
6. Click on the Save or Save and Close button.

Importing Users from LDAP

You can import users from LDAP as EGRCM users. You must first configure LDAP in the User Integration tab of the Manage Application Configurations page (page 11-3). Once that's done, complete this procedure:

1. From the Navigator, choose Setup and Administration.
2. In the Security tasks list, choose Manage Users.
3. From the Actions menu, choose Import from LDAP.
4. An Import from LDAP pop-up window lists users. Put a check mark (click) in the Select field for each user you want to import.

   Only active LDAP users who are not already created as EGRCM users are listed. If an LDAP user has the same username as an existing EGRCM user, you will not be able to import that LDAP user.
5. Click on the OK button to close the pop-up window and import the selected users.

Users imported from LDAP are at Active status and are assigned the job role of GRC User. The Source field displays LDAP if the user was imported from LDAP, or Internal if the user was created in EGRCM.

13

Managing Modules

Module Management

EGRCM has one delivered module called Financial Governance. You can create your own modules as required for your business. For example, you might want to create a module for Operational Risk Management to manage operational risks.

To create a new module:

1. From the Navigator, choose Setup and Administration.
2. In the Module Management task list, choose Manage Modules.
3. Enter a name and description for the module.
4. Specify if you want the status to be active or inactive. If, for example, you are not ready to implement the module yet, you can set it to inactive and activate it at a later date.
5. Select a template. The template defines what objects can be used for the module. The only template available currently is Standard. See "Templates Explained" for additional details about templates.
6. Select the objects you want to make available in the module.
7. To make the module easier to use, click the Relabel button to rename the objects so they suit your business objectives. Your new names appear in the Navigator.
8. Specify the relationships between the objects you selected.

Templates Explained

When creating or modifying an application module, you use a template to select and modify objects and their relationships to one another. Additional configurability can be applied through the use of user-defined attributes, perspectives, and the ability to rename, hide, or show attributes defined for each object.

There is one delivered template in EGRCM, called the Standard template. The following core objects are available for use in the Standard template:

- Six GRC base objects
- Ten risk objects

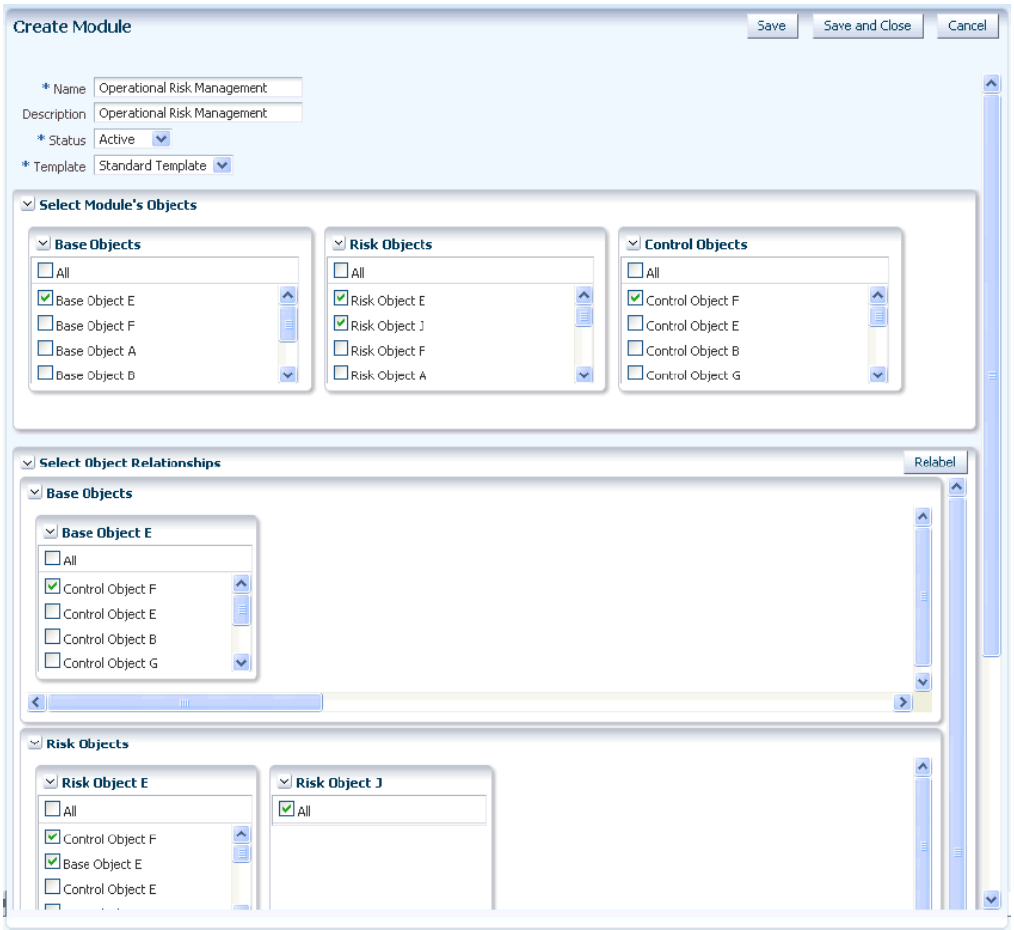
- One proposed risk
- One event
- Once consequence
- Ten control objects
- One issue object
- One remediation plan

The Standard template also supports common functionality, including perspective management, survey management, and assessment management.

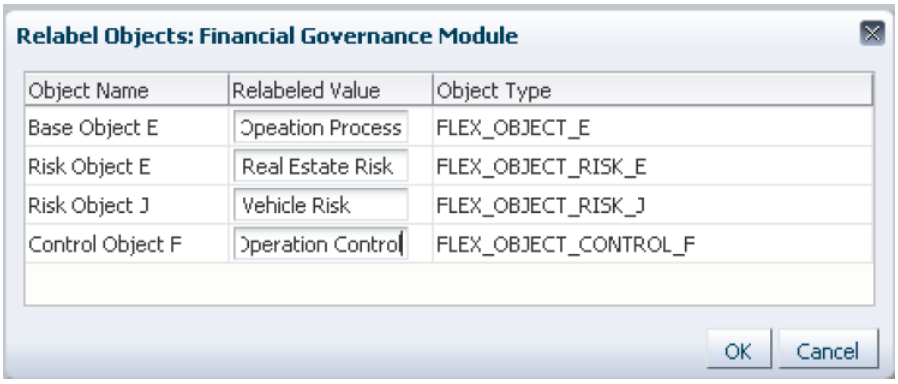
Example: Creating a New Module

In this example, a new module named Operation Risk Management is being created. This module includes:

- Base object E
- Risk objects E and J
- Control object F

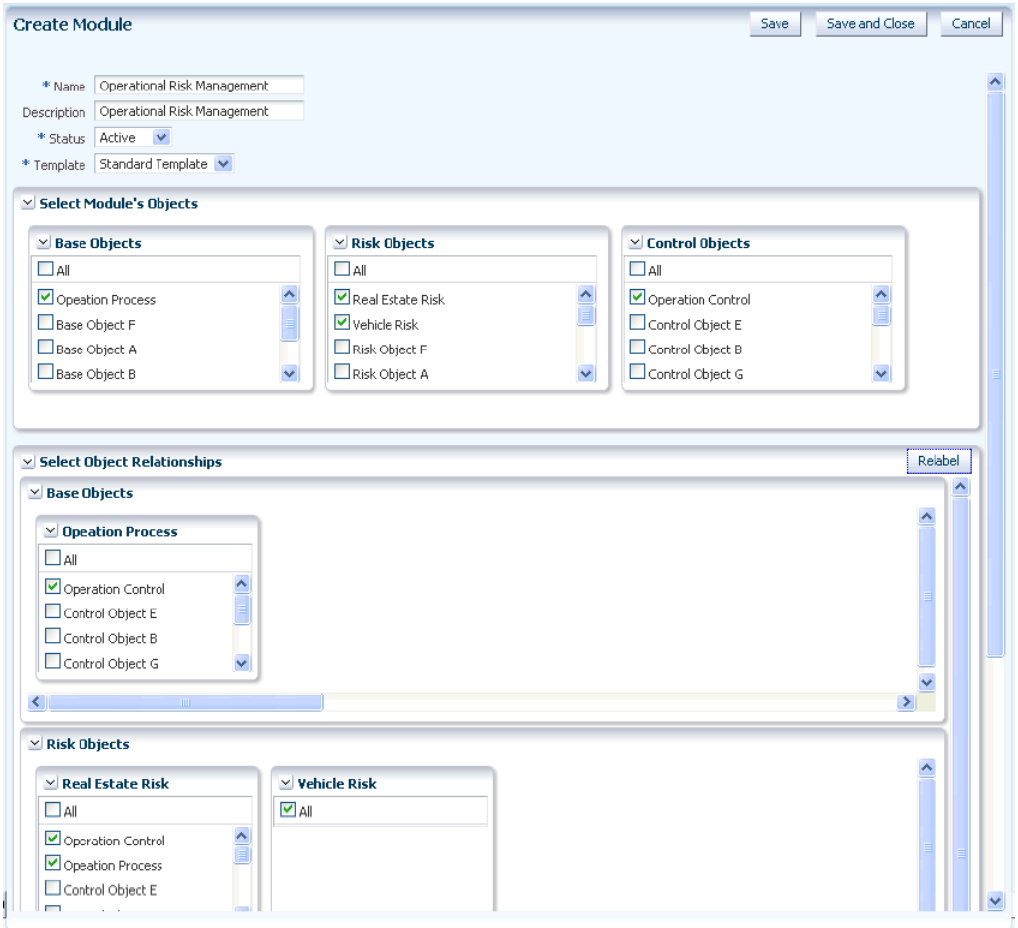


The objects have been renamed so that they are more useful. This is how they will appear in the Navigator:



The following relationships have been established between the objects:

- The Operation Process object can be related to Operation Control object.
- Real Estate Risk object can be related to Operation Control and Operation Process objects.
- Vehicle Risk object can be related to any other object available in the module.



Configuring Module Objects

You can configure module objects to show or hide features, according to your business requirements. The exact options that you can configure vary by object, but in general, you can configure the following:

- Hide: Determines whether the user interacts with events, consequences, or treatment plans. If these subcomponents are hidden, the user is never exposed to them.
- Hide Event: Hides the Event region on the Create, Edit, and Manage Risk pages. Hide Event implies hiding consequence. You can choose to hide consequences but not events.
- Hide Consequence: Events are displayed, but relationships to consequences are not displayed, within the Events region of the Create, Edit, and Manage Risk pages.
- Hide Treatment: Treatment plan, treatment, and control stratification are all hidden on the Create, Edit, and Manage Risk pages. Risk does not have a relationship to control within Risk Management. You can hide treatment plans, which implies hiding treatments and control stratification. This implies no relationship to controls.
- Hide and Default: Only applicable for treatments. Hides treatment plans and treatments but exposes related control stratification within the Manage Risk page. The system generates one default treatment plan and treatment to store the control stratification information.
- Assessment Activity Definition: Identifies which assessment activities you want to include. You can also enter additional guidance text for assessment activities.
- Activity Question: This is the question that a user is required to answer while performing an assessment.

Managing User-Defined Attributes

You can add attributes to objects such as risks, controls, base objects, perspectives, issues, assessments, and survey templates. These attributes appear automatically in the Additional Information region of the object Create, Edit, and Manage pages. When creating a user-defined attribute (UDA), you can select properties, such as data type. You can create unlimited UDAs for an object.

Depending on the data type you select for your UDA, you might have to specify:

- Display label: This is the internal identifier for the UDA and must be unique.
- Description: Enter a detailed description of how the UDA will be used.
- Data type:
  - Number
  - Date
  - String Translatable: A character string that supports translation.
  - String NonTranslatable: A character string that is not translated in codes. This is the only type that supports LOVs or value sets.
  - Link: Can be used to specify a standard URL.

- Control type: The available control types depend on the data type you have selected. They can include text box, check box, dropdown, date picker, multiple line text box. If you have chosen the Link data type, you will not see the control type option.
- Value set: For the String NonTranslatable data type, you can specify an existing value set from which users can select a value.
- Attribute name: Specify a name for the attribute. The values you can select from depend on the data type you have selected.
- URL: If you have specified the Link data type, select a URL. The URLs you can choose from are stored in the URL Repository. The link appears within the UDA Additional Details section as an active hyperlink. Refer to "Managing the URL Repository" (page 11-6) for additional details.
- Order: Specify the order in which this UDA should appear in the Additional Information field for the object.
- Assessment type: If you are creating the UDA for an assessment object, you must specify the assessment types on which the UDA will be used. You can select the Assess Risk, Audit, or Certify assessment types.
- Disabled: Choose this option if you want the UDA to exist, but not be visible to end users. For example, you might create a UDA for future use.
- Required: Choose this option if you want the UDA to be required. This means that users will not be able to save the object unless this field contains valid data.

Managing Module Perspectives

When you manage perspectives for object types, you add or delete associations with perspectives, and specify whether they are required. To associate a perspective with an object:

1. From the Navigator, choose Setup and Administration.
2. In the Module Management task list, choose Manage Module Perspectives.
3. Select the module for which you want to associate perspectives with objects.
4. Choose Create from the Actions menu, or select the Create icon.
5. Enter the following required values:
    - Name: Choose the name of the perspective.
    - Associated Object: Select the object you want to associate with the perspective.
    - Required: Specify if the user must always choose this perspective for the object. For example, you might require that a user always select the Organization perspective when he creates a new process object for the Financial Governance module. You can modify this setting later.
    - Status: Specify if this association is active or inactive. You can modify this setting later.
6. Save your changes, then click the Done button.

Managing Data Migration

You can perform one initial data import into the application. Refer to the *Oracle Enterprise Governance, Risk and Compliance Implementation Guide* for complete details of how to import data. In general, data migration includes the following tasks:

- Configure the application to suit your business requirements. This can include creating a new module (page 13-1), creating perspectives (page 3-1), configuring objects, defining UDAs (page 13-4), and managing object-perspective associations (page 13-5).
- Create the import template to manage the data you are importing. If you are importing data into the delivered Financial Governance module, a delivered template is available.
- Import the data file.

Note the following:

- The data migration process supports only an initial load, and it is a one-time process. Data load cannot be run iteratively.
- Imported data will not go through the review and approval process.
- Imported records appear immediately in the application. Their state is defined in the import template.
- The imported data log is associated with the username of the user who ran the report.

Glossary

Action Item

Detailed tasks associated with a base object that identify some type of activity to be performed.

Application Module

A specific organization of the core application's business components and business rules that is necessary to meet the requirements of a specific business initiative. Application modules are complete applications that are packaged, sold, and implemented separately, but require the EGRCM framework to run.

Assessment Activities

The type of assessment, for example design assessment, operating assessment, or certification.

Assessment Survey

A survey that is initiated from the assessment tool. Surveys are used to assist in evidence gathering for assessments and other testing.

Assessment Template

A selection of assessment activities. The assessment template also displays the user-defined component relationships and their related assessment activities.

Assessment Plan

The criteria for the assessment activities that have been associated to the assessment template.

Assessment Results

The summary of an initiated assessment and each individual object within the assessment. You can view the status and assignees of the assessment summary and each individual object within the assessment. You can view the assessment results of new and completed assessments (assessments history).

Attachment

Any type of external document that is associated with any component and its activities.

Base Object

General purpose objects that can be defined as needed.

Choice Set

A collection of answers used as a short cut for completing questions in a survey. The answers could be appropriate for many questions.

COBIT

Control Objectives for Information and related Technology is a framework that provides IT users with a set of best practices and processes to assist in developing IT governance and control.

Compliance Assessment

Assessment used to put measurements in place to determine the effectiveness of the compliance efforts. This measurement can be used as feedback to the entire compliance process to determine what further research needs to be done. This, in turn, leads to new interpretations. These interpretations feed into risk assessments and determine a different balance. They also feed into new metrics and assessments, and restart the process.

Component

The basic building block of an application module. The components represent the deconstruction of standard frameworks including COSO, COBIT, ITIL, ISO, AUSNZ, and the like. Examples include risk, control, event, issue, process, policy, and so forth.

Consequence

The outcome or impact of an event. One event can have multiple consequences, which can range from positive to negative, can be expressed qualitatively or quantitatively, and are considered in relation to the achievement of objectives.

Control

An existing process, policy, device, practice, or other action that minimizes negative risk or enhances positive opportunities. The process designed to provide reasonable assurance regarding the achievement of objectives.

Control Assessment

The systematic review of processes to ensure that controls operate and are designed effectively and appropriately.

Control Stratification

The classification of a control-to-control relationship that can be used to enhance the management of risk mitigation in a risk treatment.

Control Stratification — Key

A control that is of significant importance to the proper operation of a business process. A monitoring or subordinate control can be related to a key control. It does not have a subclass and cannot be related to a secondary control, or to another key control.

Control Stratification — Monitoring

A control that monitors one or more related controls. It is used for management assessment — for example, assessing a monitoring control but not assessing its related key control or related secondary control. It cannot be related to a subordinate control or to another monitoring control.

Control Stratification — Secondary

A control of lesser importance than a key control. It does not have a subclass. A monitoring control or a subordinate control can be related to a secondary control. It cannot be related to a key control or another secondary control.

Control Stratification — Subordinate

A control that is subordinate to one other control. The related control can be either a key control or a secondary control. It cannot be related to a monitoring control.

Control Stratification — Compensating

Controls institute additional controls to accept the risk inherent with the control weakness. The control does not duplicate its primary control; it provides coverage of some aspects of the control (assuming management approval).

Control Stratification — Mitigating

Controls that currently eliminate risk.

Control Stratification — Redundant

Controls that institute the same controls as the key control.

Corporate Communication

The underlying meaning of a regulation that is communicated to all groups and individuals. To directly issue regulations and the resources attempting to comply with the regulation.

COSO

Committee of Sponsoring Organizations of the Treadway Commission is a voluntary organization that provides guidance to executive management on GRC issues.

Data Role

The specific data to which a user with a specific job role has access.

Distribution List

A list of contacts to whom a communication or notification should be sent.

Duty Role

The lowest level within the security hierarchical structure of roles. A duty role represents the specific tasks performed with the EGRCM application, and is the role associated with specific functionality within the application.

Event

The occurrence of a particular set of circumstances, which can be certain or uncertain and can be a single occurrence or a series of occurrences.

Framework Application Module

The application foundation that provides the core services and application business components (i.e., building blocks) from which all business initiative specific application modules will be built.

Frequency

A measure of the number of occurrences per unit of time.

General Survey

Surveys are used to assist in evidence gathering for assessments and other testing. General surveys can be created and related to any object, and are created in the Survey Management tool.

GRC Business Initiative

A discreet process or set of business processes enacted to meet a particular business objective — for example, compliance with a particular law or regulation, IT governance, enterprise risk management.

GRC Intelligence

Dashboards providing business insight, including executive-level dashboards that consolidate information across initiatives as well as business-initiative-specific insight.

Guidance

A set of guidelines of help principles which assist organizations in conforming to regulation and policy enforcement. Direction or advice for a decision or course of action.

Guidance provides a set of guidelines that assist organizations in confirming to regulation and enforcing policy. Guidance can originate from external organizations separate from the policy maker or directly within the organization.

Impact

The general description of negative or positive outcome to the business objectives in the case an event occurs. For example, brand name, revenue loss, or loss of assets.

Impact Model

The criteria for weighing the significance of the events and consequences of a risk if an event occurs.

Impact Model — Qualitative

A risk-analysis method that utilizes description rather than numerical methods to define the impact of a risk (for example, *High*, *Medium*, and *Low*).

Impact Model — Quantitative

A risk-analysis method that utilizes numbers to define the impact of a risk (for example, a dollar amount).

Information Model

Identifies associated components and any tightly coupled components (such as treatments, events, or controls) used within a building block (such as a risk) in an application module.

Inherent Risk

The pure risk that is intrinsic to the specific business objective, omitting the impact of any related internal controls, established policies or procedures, or risk management practices.

Initiate Assessment

The act of selecting an assessment plan and invoking the assessment activity. Initiating an assessment allows you to review and include (or exclude) individual objects from the assessment plan selection criteria.

Issue

Reported defects or deficiencies against any business component such as risk, control, base object, or perspective item.

Job Role

The functional access and data access required for a specific job.

Legislation (Law)

The principles and regulations established in a community by some authority and applicable to its people, whether in the form of legislation or of custom and policies recognized and enforced by judicial decision.

Likelihood

The probability or frequency of occurrence.

Likelihood Model

The description or numeric weight of the probability or frequency to be applied to a risk during analysis.

Likelihood Model — Qualitative

Risk analysis method that uses descriptive rather than numerical measures to define the likelihood of risk.

Likelihood Model — Quantitative

Risk analysis method that uses numerical rather than descriptive measures to define the likelihood of risk.

Mandate

A principle, rule, or law designed to control or govern conduct, requiring compliance of some sort and usually originating externally to the organization or group to which it pertains.

Module

A collection of objects (for example risk, control, base object) configured to depict the underlying information model of the GRC solution, such as a financial compliance module.

Module Template

A template used to identify the set of objects that are necessary to solve a specific GRC business initiative (for example, process, risk, and control object types that are necessary to address a financial compliance initiative).

Module Objects

Reusable, fundamental building blocks that describe common core objects such as risks or controls.

Monitor

The action to check, supervise, observe critically, or measure the progress of an activity, action, or system on a regular basis, to identify change from the expected or required performance level.

Object Type

Identifies the individual components within the application, for example organization or person.

Perspective

Provides shape, structure, and organization for core business components (such as risks, controls, and GRC components), and supports key user activities.

Perspective Hierarchy

Defines the relationships between the perspective items. It provides structure and organization to the perspective.

Perspective Value

The individual nodes that make up the levels of a perspective hierarchy.

Policy

A plan or course of action, created by a group or organization, intended to influence and determine decisions, actions, and other matters relating to compliance of a certain external regulation. A policy refers to the approach the organization determines is necessary and sufficient to comply with the regulation.

Primary Data Role

The most granular level of data access. Contains the filters that define data access by the base attributes of the operational data. There is a primary data role for each basic action for each of the core objects within EGRCM.

Privilege

The functionality and tasks in EGRCM that are associated with a duty role.

Procedure

A manner of proceeding; a way of performing or affecting something. A set of established forms or methods for conducting the affairs of an organized body such as a business or government.

Proposed Risk

A risk that has been identified but has not yet been qualified as an actual risk.

Question Type

Identifies the possible number of responses to a survey question, and the display format for those responses.

Regulation

A law, rule, or other order prescribed by authority to control conduct.

Regulatory Audit

Helps an organization establish an audit trail of events and processes so the steps conducted for compliance purposes can be followed later. Includes the data, steps, and actions taken to ensure compliance and the history of actions or specific values to answer who, what, where, revision history, and authorized changes.

Remediation Plan

The documented response to an issue and the way progress on the resolution of the issue is tracked.

Remediation Task

An action that is included in a remediation plan that is used to resolve an issue.

Revision Date

The date on which an object was last modified.

Risk

The chance of something happening that will have an impact on objectives. A risk is often specified in terms of an event or circumstance and the consequences that may flow from it. Risk is measured in terms of a combination of the consequences of an event and their likelihood. Risk may have a positive or negative impact.

Risk Analysis

The systematic process to understand the nature of risk and to reduce its level. Risk analysis can provide a basis for risk evaluation and decisions about risk treatment.

Risk Context

Enables organizations to define the general parameters for how risks must be managed and the scope for the enterprise risk management process. Risk context should include the organization's external and internal environment and the purpose of the risk management activities.

Risk Analysis — Qualitative

The process of examining risk characteristics by descriptive measures rather than numerical criteria. Qualitative analysis can be performed as an initial analysis of risk prior to further detailed analysis.

Risk Analysis — Quantitative

The process of examining risk characteristics by numerical measures such as revenues, earnings, margins, and market share.

Risk Analysis Model

The technique designed to quantify the impact of risk uncertainty.

Risk Assessment

The appraisal of the risk definition and inventory of systems and the business processes they support; an assessment of potential vulnerability and threat; a decision to act or not; evaluation of the effectiveness of the action; and communication about decisions made.

Risk Criteria

The terms of reference by which the significance of risk is assessed. Risk criteria can include associated cost and benefits, legal and statutory requirements, socioeconomic and environmental aspects, the concerns of stakeholders, priorities and other inputs to the assessment.

Risk Evaluation

The process of comparing the level of risk against risk criteria. This process assists in decisions about risk treatment.

Risk Identification

The process of determining what, where, when, why, and how an event could occur.

Risk Impact — Inherent

The probability of loss arising out of circumstances or due to the existing environment.

Risk Impact — Residual

The remaining aspects of an event after implementation of risk treatment.

Risk Impact — Target

The acceptable level of loss arising out of an event occurring. This is the goal an organization tries to achieve.

Risk Level

The degree of chance an event will occur and will have an impact on business objectives.

Risk Treatment

The process of selection and implementation of measures to modify a risk. Risk treatment measures can include avoiding, modifying, sharing, or retaining risk.

Risk Class

The business objectives classification of a risk.

Security Roles

Refers to roles given a user to grant access.

Stakeholder

The people and organizations who may affect, be affected by, or perceive themselves to be affected by a decision, activity, or risk.

Stakeholder — External

The people and organizations external to the main organization who may affect, be affected by, or perceive themselves to be affected by a decision, activity, or risk.

Stakeholder — Internal

The people and organizations internal to the main organization who may affect, be affected by, or perceive themselves to be affected by a decision, activity, or risk.

State

The current condition of an object — for example, new, open, or closed.

Survey

A collection of facts, figures, or opinions used in evidence gathering. Surveys can be used within an initiated assessment as supporting documents of the assessment.

Test Instruction: Automatic

Test steps that are performed in an external automated tool.

Test Instruction: Manual

Test steps that are performed with human intervention.

Test Plan

Documents the steps required to perform a control test.

Treatment

The action or plan that will be used to mitigate a risk.

Treatment Plan

A collection of decisions and mitigating actions (both present and future) that will be implemented to mitigate a risk.

Treatment Stratification — Compensating

A treatment that institutes additional controls to accept the risk inherent with the control weakness. Does not duplicate its primary control; it provides coverage of some aspects of the control.

Treatment Type — Risk Avoidance

A decision not to become involved in a risk situation, or an action to withdraw from it.

Treatment Type — Risk Reduction

Actions taken to lessen the probability, negative consequences, or both associated with a risk.

Treatment Type — Risk Sharing

Sharing with another party the burden of loss, or benefit of gain, of a risk.

User

A person who requires access to EGRCM.

User-Defined Attribute (UDA)

User customizations that provide additional classification or other clarifying information to an object.

User Profile

The description of a person who requires access to EGRCM, including personal information (such as name) and security information (such as job role).

Voluntary

When an organization has a regulatory entity within it that imposes standards to which the organization is required to adhere.