Oracle® Enterprise Governance, Risk and Compliance Manager

User Guide

Release 8.6.4.5000

Part No. E38967-02

March 2013

ORACLE

Oracle Enterprise Governance, Risk and Compliance Manager User Guide

Part No. E38967-02

Primary Author: David Christie

Contents

7 Survey Management

Preface

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

An Oracle Enterprise Governance, Risk and Compliance (GRC) platform hosts several products — Oracle Application Access Controls Governor (AACG), Oracle Enterprise Transaction Controls Governor (ETCG), and Oracle Enterprse Governance, Risk and Compliance Manager (EGRCM).

The GRC platform runs modules. "Financial Governance" is the name of an EGRCM module, and users may create other EGRCM modules. "Continuous Control Monitoring" (CCM) is the name of the module in which AACG and ETCG run. (Moreover, GRC "Tools" offer functionality used across GRC modules.)

This *Enterprise Governance, Risk and Compliance Manager User Guide* covers features specific to EGRCM. (Other product-specific user guides cover features particular to AACG and to ETCG.)

An *Enterprise Governance, Risk and Compliance User Guide* covers most functionality common to the GRC applications (although the *Enterprise Governance, Risk and Compliance Installation Guide* covers some setup and administration topics). Refer to these guides as well as the EGRCM user guide as you use EGRCM.

Additionally, implementation guides discuss concepts you should consider as you set up GRC products for use. One implementation guide exists for each of AACG, ETCG, and EGRCM, and a distinct implementation guide covers GRC security. Consult these documents as you begin to use GRC.

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 strategy for addressing risk and complying with regulatory requirements.

EGRCM consists of modules running within an Enterprise Governance, Risk and Compliance platform. 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. They may also create user-defined attributes — information added to a given object to extend its definition.

Users may create perspectives, each of which is a set of hierarchically arranged values. Each represents a context in which processes, risks, controls, and other objects exist. Users can relate individual perspective values to individual objects, thus cataloging them by organization, region, or any other concept the company finds meaningful. Perspective values also play a part in GRC security.

EGRCM enables users to perform periodic assessments of objects, to determine that they are defined and implemented correctly when they are created, or that their definition and implementation remain appropriate as time passes. 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

Object is a generic term for any of the components one may include within a module to achieve GRC goals, such as base object, risk (along with event, consequence, treatment plan, and treatment), and control (along with test plan, test instruction, and test step).

The template from which you create a module determines the relationship each object may have to other objects. Within the template, a base object is typically the focus

of GRC efforts, and other objects refer to it. For example, the Financial Governance module uses one base object, configured as "Process"; it represents business processes in which users identify risks and create controls to mitigate those risks.

Users may create multiple instances of each object included within a module — for example, any number of Financial Governance business processes, or any number of risks inherent to a given process.

Reporting

From Reports Management pages, users can run reports concerning EGRCM, its companion applications, and GRC administration. Those that apply to EGRCM provide information about risks, controls, assessments, and issues, among other topics. Because Report Management features are common to all GRC applications, they are discussed in the *Oracle Enterprise Governance, Risk and Compliance User Guide*.

Common Procedures

As you work with EGRCM objects, you may perform certain procedures that are common to GRC applications. You may use a home page or overview pages to view worklists (records of tasks requiring action on your part) and notifications (records of tasks in which you have an interest, but which do not require you to act). You may use navigation features to move among GRC application pages. You may use search features to filter lists of records. You may set "user preferences" — review and edit information about your user account. For complete information on these features, see the *Oracle Enterprise Governance, Risk and Compliance User Guide*.

Descriptions of other common procedures follow.

Reviewing or Approving Objects

EGRCM workflow may require that objects be reviewed or approved after they are created or modified. If you have the appropriate job role to complete such a task, it appears among your worklists. You have these options:

- Accept the object as it is. If you are reviewing an object for which approval is required, an approval task appears on the worklist of appropriate users. If you are reviewing an object for which approval is not required, or if you are completing an approval task, the object's state is set to Approved.
- Request information. The object remains in its current state (In Review or Awaiting Approval), and a new entry appears on the worklists of appropriate users, notifying them that more information is requested. (While one reviewer or approver awaits information, another can complete his review.)
- Reject the object. This removes the object from the workflow. The user who created or modified the object is notified.
- Cancel your review: This leaves the object in its current state, unchanged.

Selecting Perspectives

You can assign perspective values to risks, controls, and base objects (processes in the Financial Governance module). These may serve as filtering values in object-management pages or in reports. They also play a part in determining which users have access to any of these objects — those whose job roles contain data roles associated with perspective values that match the values selected for the object. (Users must also have duty roles granting privileges to work with the object).

Although perspective hierarchies are created in Perspective Management, each hierarchy becomes available for use with an object only after it has been associated with that type of object in Manage Module Perspectives. In each object view, creation, or edit page, a Perspectives panel displays a tab for each perspective hierarchy that has been associated with the object.

In Manage Module Perspectives, a perspective may be designated as required for the object with which it is being associated. If so, the tab that displays its name also displays an asterisk; a user is unable to save an instance of the object if he does not select a value for the required perspective.

For more information on creating or editing perspectives, or associating them with object types, see the *Oracle Enterprise Governance, Risk and Compliance User Guide*.

To assign perspective values to an object:

1. In an object creation or edit page, click on the tab for the perspective hierarchy from which you want to select values.
2. In an Available Perspective Items list, choose one or more values you want to assign to the object. Or, in a Selected Perspective Items list, choose values you want to remove from the object. (Ultimately, values are assigned to the object if they appear in the Selected list.) Do any of the following:
   - Click on an icon next to the root node to expose perspective values at the next hierarchical level. Click on the icon next to a node at that level to reveal its child nodes. Continue until you reach the node you want.
   - Use View options to display, and choose among, nodes. Select View > Expand All to display all nodes configured for the perspective. Other View options enable you to collapse the entire hierarchy, expand or collapse nodes beneath a selected node, display only a child node and those that descend from it, and scroll to the first or last node.
   - Type a text string in the search box to produce a list of matching perspective-value names. You can use the percent sign (%) as a wild-card character; entries are not case-sensitive. A search returns only matching perspective values; it does not display an entire perspective hierarchy.

   Then to choose one perspective value, click on it. To choose a continuous set, click on the first, hold down the Shift key, and click on the last. To choose a discontinuous set, hold down the Ctrl key as you click on values.
3. Click the > button to cause values chosen in the Available list to appear in the Selected list. Or, click the < button to remove values chosen in the Selected list from that list.

(Alternatively, click the >> button to place all perspective values in the Selected list, or the << button to remove all values from that list.)

4. Repeat steps 1–3 to select any number of perspective values from any number of hierarchies.

As you assign perspective values, you may also select a View Perspective button to see a representation of the full hierarchy from which you are selecting a value. Click on any value, and a Related Components panel opens, displaying objects with which the value is associated. You can view all objects, or filter by process, risk, or control.

Selecting Related Objects

You can define parent-child relationships between objects. For example, in the Financial Governance module a risk can be related to the process in which the risk may have an effect (in which case the process is the parent of the risk). Or, a control may be related to the risk it is meant to address (in which case the risk is the parent of the control). In general, you can create new relationships to children of an object with which you are working, or view existing relationships for both child and parent objects.

A page displaying a record of an object also displays a Related Objects grid. The behavior of this grid varies depending on the type of page you are using:

- In a manage- or edit-object page, you can view objects already related to the object with which you are working. Each appears as a row in the Related Objects grid. In a manage-object page, the name of each related object is a link to the manage page for that object (although the link is active only if your roles grant access to the related object).
- In a create- or edit-object page, you can create new relationships. From an Actions menu in the Related Objects grid, you may select either of two options:
  - Add opens a pop-up window displaying a list of objects. You can use standard search features to locate the object you want. Click on that object, then on the Ok button. That object then appears as a new row in the Related Objects grid.
  - Create opens a pop-up window displaying an instance of the window in which an object can be created. Complete fields in this window (as instructed elsewhere in this guide), and save or submit the object. The object then appears not only in the Related Objects grid, but also in the manage pages for the type of object you've created.

Within a Related Objects grid, rows for each type of object appear in their own tabbed listing. The tab for a given object type appears only when appropriate. In the Financial Governance module, for example, a Process tab does not appear if you are working with a control, because a control does not have a direct relationship to a process.

Attaching Files

In each of the pages in which you create or edit objects, you can attach files to them. An attachment may, for example, be a text file, spreadsheet, or web site that provides more information about an object than can be contained in its Description field.

For most attachments, you need to specify a content type. These values are configured in Manage Content Types, which is available in the Setup and Administration tasks. If no existing content type is appropriate for your attachment, have one created in Manage Content Types (see the *Oracle Enterprise Governance, Risk and Compliance User Guide*).

To attach a file:

1. Click on the green plus sign next to the Attachment label in a create or edit page. An Attachments pop-up opens.
2. Select Actions > Add. A new row appears.
3. Select a Type — desktop file or url.
4. If you select desktop file, click the browse button to navigate to, and select, the file you want. Select a content type, compose a title, and optionally enter a description.

   If you select url, enter it in the File Name/URL field, compose a title, and optionally enter a description. (Content type does not apply in this case.)
5. If you wish to create additional attachments, repeat steps 2 through 4 for each attachment.
6. Click the OK button to exit the Attachments pop-up.

You can also delete an attachment by opening the Attachments pop-up, selecting a row, and selecting Actions > Delete.

To view an attachment, click on its name in the management, creation, or edit page for an object.

Reviewing Incident Results

Users of Oracle Application Access Controls Governor (AACG) or Enterprise Transaction Controls Governor (ETCG) may create "continuous controls." These either define conflicts among duties that can be assigned in a company's applications, or define ways in which transactions entail risk. Continuous controls generate "incident results" — records of transactions, or users with access, defined as risky by a continuous control. (AACG and ETCG run as a Continuous Control Monitoring module, or CCM, in the Enterprise Governance, Risk and Compliance platform.)

Processes (or base objects), risks, or controls within the Financial Governance module or custom modules may display incident results generated in the CCM module. This happens if users employ "Relationship Assignment" features in the CCM module to relate incident results to objects in other modules.

To view incident results related to an EGRCM object, open the Manage page for a process, base object, risk, or control. Click on its Results tab. However, for you to see incidents, your roles must grant access not only to the object to which incidents are related, but also to the incidents themselves. Moreover, the Results tab is available to an object only if it is selected for that type of object in Setup and Administration > Module Management > Configure Module Objects.

Within the Results tab of an EGRCM object, incident results are available for viewing only; they cannot be edited. (Users may set the status of incident results or edit them only in the CCM module.) Within the Results tab, you can hide or restore

the columns that appear in the grid displaying incidents; right-click in the header row of the grid to open a checklist of columns. These include the following:

- Status: By default, incidents appear at an Assigned status, which means that one or more "result investigators" have been designated to address them. Those investigators may reset status to Accepted (nothing need be done to resolve the incident), Remediate (some action must be taken to resolve the incident), or Resolved (remedial action is confirmed to have been carried out).

  GRC may set other statuses. Authorized is given to incidents that result from "preventive analysis" in AACG. A control violation may cause the assignment of a role to a user to be suspended. If a result investigator then approves the assignment, and the control is subsequently run, incidents related to the assignment receive Authorized status.

  Control Inactive means that an incident is no longer of concern because the control that generated it has been inactivated. Closed indicates that because an incident has been resolved in the business-management application, a subsequent evaluation of controls finds that the incident need no longer be addressed.

- State: GRC assigns states to incident results depending upon whether they were saved or submitted at a given status. Typically (but not necessarily) an incident's state is In Investigation if its status is Assigned or Remediate, Approved if its status is Accepted or Resolved, or Closed if its status is Closed or Control Inactive.

- Incident Information

  – For an access incident, this is a path through which a user, assigned access points that a control defines as conflicting, can reach one of those access points.

  – For a transaction incident, this is the value of the first attribute among those selected to characterize the suspect transaction. (These values were selected during configuration of a model that served as the basis of the continuous control that generated the incident.)

- Group and Grouping Value fields

  – For an access incident, the Group field identifies pairs of access points. Every pair includes the access point identified in the Incident Information field (at the path specified in that field). Each pair also includes an access point assigned to the user (via a specific path) that the control defines as conflicting with the Incident Information access point. There may be any number of pairs. For access incidents, the Grouping Value field is blank.

  – For transaction incidents, results vary: If a transaction control uses a filter to find transactions with similar values for a specified attribute, the Group field displays the word *Similar* and the specified attribute, and the Grouping Value field displays the value of that attribute for a given incident. If a transaction control uses a function to calculate a value for a specified attribute across a group of transactions, the Group field identifies the calculation (count, sum, or average) and the specified attribute, and the Grouping Value field displays the calculated value for a given incident. If a transaction control uses a pattern to create a baseline value, the Group field

displays the pattern type and the attribute upon which the pattern is based, and the Grouping Value field displays the baseline value.

Other incident values are self-explanatory.

Saving or Submitting Objects

As you create or edit objects, you may choose to save or submit them. Each object may exist in any of a variety of "states"; saving a new object places it in a New state, while submitting it advances it to another state in your workflow. Users' access to data is granted by their roles, which in part specify the state in which data exists, so submitting an object places it in the appropriate state for other users in your workflow to see it. Typically you would save an object if you intend to work on it further before making it available to others, and submit it when it is ready for use by others. If, for example, your workflow calls for review and approval of objects, submitting an object would place it in a state that makes it available for review or approval.

Note that an object may be deleted only if it is in the New state. Once an object has been submitted, it can no longer be deleted.

It is assumed that although you may choose at first to save an object, your final action will be to submit it so that it is active in your system.

To save an object, you may select a Save button; if so, the page in which you create or edit the object remains open and you may edit the object further. Or you may select a Save and Close button (available in a drop-down field accompanying the Save button); if so, the create or edit page closes and the overview page opens. To submit the object, click on the Submit button; the create or edit page closes, and the manage (view) page for the submitted object opens.

2

Risk Management

An EGRCM risk defines circumstances which, if they were to occur, would materially affect your business. To work with a risk is not only to define it, but also to "analyze," "evaluate," and "treat" it:

- Analysis is a first step in understanding the risk itself and the impact of steps you take to mitigate it. This process uses an "analysis model," which in turn specifies two other models: A "likelihood model" expresses the chance that the potential risk will actually occur. An "impact model" expresses the potential damage if the risk were to occur. The analysis model consolidates likelihood and impact values into overall results. When used for analysis, the models produce "inherent" results — levels of risk existing before any mitigation is in place.
- Evaluation considers the risk itself, and uses a "context model" to do so. This model defines "risk criteria." For each criterion, the model establishes a set of "tolerance" standards, which enable the model to return recommendations to accept, monitor, or treat risk. The context model also returns an overall "risk rating," and it specifies a "significance model," which in turn assigns a value that rates the importance of the risk in comparison with other risks.
- Treatment continues the process of weighing the impact of remediation steps upon a risk. Like analysis, it uses the analysis, likelihood, and impact models, which may now return "residual" or "target" results — levels of risk existing after controls are defined, or expected over time as the result of a treatment plan. (Your company may configure the risk object to use "related controls" or formal "treatments," and target results apply only in the latter case.)

You may choose to analyze or evaluate a given risk, or both. If you choose to do both, it's recommended that you analyze first, because inherent results are displayed, and may be taken into account, during evaluation.

Inherent results are directly comparable with residual or target results, because all are produced by the same set of models. You may determine, for example, that residual results for a risk are better than its inherent results, and so controls are successful in mitigating it. Or you may discover that residual results are poorer, and so existing controls are insufficient to mitigate the risk.

In any case, results returned by each of these operations are meant to be compared with one another, and typically a page in which one set of results is generated also displays other types of results.

For the Financial Governance module, EGRCM provides seeded context, analysis, significance, likelihood, and impact models. Owing to a limitation in the export process, it's recommended that you not use the seeded models directly; you can, however, create copies of them and use the copies. Or, you can create your own models.

As you work with a risk, you can relate it to controls meant to address it. Depending on how your company has configured the risk object, you may also be able to define "events" (specific circumstances under which the risk may manifest itself), "consequences" of the events, and treatment plans to limit risk.

Working with Risk Models

While analyzing or evaluating a risk, a user enters certain values that serve as inputs to risk models, which then work together to produce other results. To work with the models themselves, you need to understand how values output by some models serve as inputs to other models. To begin with, the likelihood and impact models produce inputs to the analysis model, and the context model produces a risk rating that both has value in itself and serves as an input to the significance model.

Likelihood and Impact Models

Each of the likelihood and impact models correlates text labels with numeric values. The models may be "qualitative" or "semi-quantitative." A qualitative model associates each label with a specific number — for example, Low = 2, Medium Low = 4, Medium = 6, Medium High = 8, and High = 10. A semi-quantitative model associates each label with a numeric range — for example, Low = 1–25, Medium = 26–75, and High = 76–100. (The seeded models are qualitative.)

If a risk uses qualitative models, a user who analyzes the risk selects one likelihood label and one impact label. The two models then supply corresponding numeric values to the analysis model, which uses them to calculate an overall risk level.

If a risk uses quantitative analysis, a user selects a number to rate each of likelihood and impact. (The user also selects a timeframe value for likelihood; see the discussion of the analysis model.) The semi-quantitative likelihood and impact models apply corresponding labels; the analysis model uses the numeric values to calculate overall risk.

To create (or edit) likelihood or impact models, select Manage Likelihood Models or Manage Impact Models under Risk Administration — Risk Analysis in the Risk Management Tasks. Select the model type and provide the labels and numeric values required by the type you select.

Analysis Model

An analysis model specifies a likelihood model and an impact model, accepts numeric values supplied by those models, and uses them in a formula that calculates a single numeric risk score. How this score is calculated and used depends on whether the analysis model is "qualitative" or "quantitative." (The seeded model is qualitative).

A qualitative model maps ranges of scores to labels, and selects as an overall risk level the label that corresponds to the risk score it calculates. To arrive at that score, it multiplies the values supplied by the likelihood and impact models.

For example, imagine that while analyzing a risk, a user selects Medium Low as a likelihood and Medium High as an impact, and the likelihood and impact models correlate these labels to the values 4 and 8. The qualitative analysis model would use these values to calculate the number 32. Further, if the risk level mapping of the analysis model were to correlate the values 21–40 with the label "Medium Low," then that label would be selected as the overall risk level.

A quantitative analysis model returns the numeric score it calculates as the overall risk rating. To arrive at that score, it may use either of two formulas:

- A "product" formula states *Risk level = Likelihood × Timeframe factor × Impact*.
- A "weighted product" formula states $Risk\ level = (Impact \times Weighting\ Factor)^X \times (Likelihood \times Timeframe\ factor)^Y$.

For the weighted product formula, a user supplies the weighting factor and X and Y powers as he creates the model. For either formula, another user sets the timeframe as he performs analysis on a risk. He selects one in a set of labels, which correspond to numeric values as follows: Day = 365.25, Week = 52.18, Month = 12, Quarter = 4, Year = 1, Decade = 0.1, and Century = 0.01.

To create (or edit) an analysis model, select Manage Analysis Models under Risk Administration — Risk Analysis in the Risk Management Tasks. Then:

- Select the model type, and the likelihood and impact models that will provide input values. You must select qualitative likelihood and impact models for a qualitative analysis model, or semi-quantitative likelihood and impact models for a quantitative analysis model.
- If you are creating a qualitative model, create the risk-level mapping: create labels that describe overall risk levels, and correlate each with a range of risk scores.
- If you are creating a quantitative model, choose whether to use a product formula or a weighted product formula; for the latter, enter values for weighting factor and the two exponents. The weighting factor is a percentage: if you enter the value 1, for example, the formula will use the value 0.01.

Significance Model

A significance model correlates text labels with ranges of risk ratings. It accepts as inputs the risk ratings calculated by a context model. For each risk, it then selects as an overall risk significance the label that corresponds to the risk rating calculated by the context model.

To create (or edit) a significance model, select Manage Significance Models under Risk Administration — Risk Evaluation in the Risk Management tasks. Create significance labels (such as Low, Medium, High) and assign a range of risk ratings to each label. (The higher a risk-rating score, the greater the risk.) Risk ratings range from 1–100.

Context Model

A context model sets any number of criteria by which a risk may be judged. The seeded Financial Governance Context model, for example, creates Effectiveness,

Reliability, and Compliance criteria. For each criterion, a context model assigns a set of labels, which may be numeric or textual. The model correlates each label with:

- A tolerance value — Accepted, Monitor, or Treat. These are recommendations of how to deal with the risk. A given tolerance value may be assigned to more than one label. Each of the three tolerance values should be assigned at least once for each criterion.
- A rating — a numeric value that serves as a risk score. Values range from 1–100, although not every one of those values need be assigned. The higher the number, the greater the risk.

While evaluating a risk, a user will select one of the labels created for each criterion. The context model then assigns to that criterion the tolerance value and the rating associated with the selected label. Of the tolerance values selected for all criteria, the risk assumes the one that requires the most active response. Moreover the model calculates an overall risk rating — the average of the individual criteria ratings.

To create (or edit) a context model, select Manage Context Models under Risk Administration — Risk Evaluation in the Risk Management tasks. Select the significance model that will use the overall risk rating as an input. In a Risk Context Details section, name each of the criteria by which the context model will judge risks. Click on each criterion in the Risk Context Details area to refresh a Risk Criteria Details section; in that section, set label, tolerance, and rating values for each criterion.

Creating a Risk

To create a risk, select Create New Risk among the risk-management tasks. (Or select Actions > Create Risk from the Manage Risk page.) A Create New Risk page opens:

In this page:

1. Enter values in the Risk Details panel.
    - Enter a name and a description. These fields record what is risky about the risk you are creating. The name, for example, might be "Earthquake," and the description might be "Earthquake shuts down production at factory."
    - Select context and analysis models.
    - Select a currency in which monetary amounts affected by the risk are expressed. Also select a type. (Values available in the Type LOV are created at the Manage Lookups page, available in the Setup and Administration tasks. If no existing type is appropriate for the risk you are creating, you may have a new type created in the Manage Lookups page. See the *Oracle Enterprise Governance, Risk and Compliance User Guide*. However, a type value is optional.)
    - Optionally, attach files to the risk (see page 1-4).
    - Type comments, if any are germane.
2. If user-defined attributes have been created for the risk object, fields representing these UDAs appear in an Additional Details panel. Provide values for these fields.

3. In the Perspectives panel, select perspective values appropriate to the risk (see page 1-3).
4. In the Related Objects panel, select controls meant to address the risk (see page 1-4).
5. If your company uses events and consequences, select events appropriate to the risk in the Events panel. (Depending on how your company has configured the risk object in Administration > Module Management, this panel may not exist.)
6. Save or submit the risk (see page 1-7).

Managing Risks

From a Manage Risk search page, you can display a summary list of existing risks (using standard search features to filter them). You can create a new risk. You can select a risk and edit, copy, or delete it. To open the Manage Risk search page, click on Manage Risk in the Risk Management tasks.

From a Manage Risk page specific to a selected risk, you can view or edit risk details; conduct inherent risk analysis or perform risk evaluation, and view the results of past analyses and evaluations; relate controls to the risk and determine residual risk values; or assign treatment plans to the risk and determine target risk values. You can also assess the risk (see page 6-1), create or review an issue against it (see page 5-1), or (potentially) review incident results assigned to it (see page 1-5). To open the Manage Risk page for a specific risk, click on its name in the Manage Risk search page.

Editing, Copying, or Deleting Risks

From the Manage Risk search page, click in the row for a risk. Then do any of the following:

- Edit the risk. Select Actions > Edit Risk (or the edit icon), and an Edit Risk page opens. It's laid out similarly to the Create Risk page, and in general you can modify risk values in the same way as you create them. (Another way to open the Edit Risk page is to click an Edit Risk button in the Definition tab of the risk-specific Manage Risk page.)
- Copy the risk, as a template for the creation of a new risk. Select Actions > Copy Risk, and Create New Risk page opens, populated with values for the risk you've copied. Modify them as you would if you were editing a risk.
- Delete the risk. Select Actions > Delete Risk (or the delete icon). A confirmation message appears; click on its OK button. (A risk can be deleted only if its state is New — if it has been saved, but not submitted. If a risk cannot be deleted, the Delete Risk option is disabled.)

Viewing Risk Details

From the Definition tab of the risk-specific Manage Risk page, a Risk Details section displays the values configured for a risk as it was created or edited. (Other tabs in this page also present risk details.) You can view or create comments (to do the latter, click the Add Comments button). You can view, but not modify, the perspec-

tive values assigned to the risk, and the controls and processes related to the risk. If your risk object has been configured to use events and consequences, you can view, but not modify, the events and consequences associated with the risk. You can also view a Risk Analysis Map, which presents graphically the most recent inherent and residual risk results.

Inherent Risk Analysis

From the Analysis tab of the risk-specific Manage Risk page, a Risk Analysis panel presents a row for each inherent-risk analysis. Click on a row to display complete details of the analysis it represents. Likelihood and impact values were selected by the user who performed the analysis, and an overall risk level was calculated by risk models. "Inherent" values are those that would apply if the risk were not mitigated by any controls or treatments. A Risk Analysis map displays the most recent inherent and residual levels calculated for the risk, and a Risk Analysis graph displays each overall risk level — inherent and residual — calculated for the risk, arranged by date.

To conduct a new inherent-risk analysis:

1. Select Actions > Create (or the create icon) in the Risk Analysis panel, or Actions > Create Analysis near the upper right corner of the page. A Create Analysis page opens. In it, the analysis model configured for the risk is selected (and cannot be changed).
2. In the Analysis Details area, type a description. (This may, for example, be an explanation of how changed circumstances justify a new analysis, when one has already been conducted.)
3. Enter a due date. (You may be setting up an analysis to be completed later, and at that point enter a separate target completion date if it will differ from the due date.)
4. In the Likelihood section of the page, select a likelihood model and a value configured for that model. (If the model is qualitative, this value is a label such as "Medium" or "High"; if the model is semi-quantitative, the value is a number, with a higher number representing a greater likelihood of the risk occurring.)
5. In the Impact section, select an impact model and a value configured for that model. (Again, if the model is qualitative, this value is a label; if the model is semi-quantitative, the value is a number, with a higher number representing a greater impact.)
6. Select Save or Save and Close.

(See "Risk Overview" and "Work with Risk Models" for explanations of how the models you select will produce analysis results.)

The analysis is saved in an In Edit state. To complete the analysis, select its row, then select Actions > Edit in the Risk Analysis panel. An Edit Analysis page opens; in its Actions menu, select Mark as Complete.

Risk Evaluation

From the Evaluation tab of the risk-specific Manage Risk page, a Risk Evaluations panel presents a row for each past risk evaluation. Click in a row of the grid to display complete details of the evaluation it represents: A user will have selected a value for each risk criterion established by the context model assigned to the risk. From those values, models will have calculated a tolerance and rating for each criterion, an overall risk rating, an overall tolerance (labeled "Evaluation Result"), and a significance. (See "Risk Overview" and "Work with Risk Models" for explanations of how risk models produce evaluation results.) A Risk Significance by Criteria bar chart shows the rating for each criterion in the most recently completed evaluation.

To perform a new evaluation:

1. Select Actions > Create (or the create icon) in the Risk Evaluations panel, or Actions > Create Evaluation near the upper right corner of the page. A Create Evaluation page opens, displaying risk details and information about the most recent analysis and treatment undertaken for the risk. An Evaluation Details panel displays the context model configured for the risk (which cannot be changed).
2. In the Evaluation Details panel, supply evaluation notes (which may, for example, explain why the evaluation is being conducted).
3. Enter a due date. (You may be setting up an evaluation to be completed later, and at that point enter a separate target completion date if it will differ from the due date.)
4. Select or clear the Catastrophic check box. Selecting it sets the risk rating to 100 (its maximum value), evaluation results to Treat, and risk significance to High. Clearing it allows these values to be calculated by the context and significance models.
5. The Risk Criteria panel displays a row for each criterion established by the context model. For each, select a value established by that model. (The higher the value, the greater the risk.) For each, the context model provides a corresponding tolerance and rating.
6. Click on Save or Save and Close.

The evaluation is saved in an In Edit state. To complete the evaluation, select its row, then select Actions > Edit in the Risk Evaluations panel. An Edit Evaluation page opens; in its Actions menu, select Mark as Complete.

Related Controls and Residual Risk

Depending on how your company has configured the risk object in Setup and Administration > Module Management, the risk-specific Manage Risk page displays either a Related Controls tab or a Treatments tab.

If your company uses Related Controls, the page available from this tab displays (in addition to risk details and values for the most recent inherent-risk analysis) a list of controls meant to mitigate the risk, as well as "stratification" values that depict how the controls work together. The page also includes a Control Impact panel, which displays residual likelihood, impact, and risk — values that apply after the related controls have had their effect upon the risk.

To add or remove related controls, set their stratification values, or determine residual risk values, click the Edit Related Controls button, or select Actions > Edit Related Controls near the upper right corner of the page. An Edit Related Control Activity page opens.

To add a control, do either of the following:

- Select Actions > Add Primary in the Related Controls panel. Or click the Add Primary Control button.
- Click in the row for an already-selected control, and select Actions > Add Subordinate. Or click the Add Subordinate Control button. A subordinate control is placed beneath, and indented to the right of, the already-selected control.

An Add Control pop-up window opens. In it, search for and select the control you want to relate to the risk. (To remove a control, click in its row in the Related Controls panel and select Actions > Remove.)

Next, select a stratification value for each related control. These include:

- Key: A control of significant importance to the operation of a business process.
- Monitoring: A control that monitors one or more related controls.
- Compensating: A control that addresses weakness in a related control.
- Redundant: A control that implements the same regulation as a key control.
- Mitigating: A control that serves to eliminate risk for a process.

To perform residual analysis, use fields in the Control Impact panel of the Edit Related Control Activity page. Select a likelihood value in the Residual Likelihood field, and an impact value in the Residual Impact field. These fields accept values configured for the likelihood and impact models selected for use with the risk; these values feed the analysis model associated with the risk to produce an overall residual risk value. (See "Working with Risk Models," page 2-2.) Residual risk values are not only displayed in the Related Controls page, but also charted in the Risk Analysis Map on the Definition page and in the Risk Analysis graph on the Analysis page.

When you finish making changes in the Edit Related Control Activity page, save or submit the risk (see page 1-7).

Treatments and Target Risk

If your company has configured the risk object to use treatments, the risk-specific Manage Risk page displays a Treatments tab. The page available from this tab presents risk details, a treatment summary, and a list of treatment plans. The Treatment Summary panel consists of values for inherent risk, residual risk, and target risk (the risk level you expect to achieve over time through treatment), as well as treatment cost. The Treatment Plans panel lists existing treatment plans (if any); you can click on any of the plans in this list to view its details.

In this page, click an Edit Treatment button (or select Actions > Edit Treatment) to open an Edit Risk Treatment Activity page. This also presents the treatment summary, but enables you to select target-risk values. To do so (as for residual values),

you select a likelihood and an impact model, then select a value for each of these models. This page also includes a list of treatment plans; in it, however, you can select the Create option from an Actions menu to create a new plan; select an existing plan and choose the Edit option from the Actions menu to modify the plan; or select a plan and choose the Delete option from the Actions menu to remove the plan.

If you choose to create or edit a plan, a page opens for that purpose. In it, enter (or modify) a name and description, and select a Usage value: In Use indicates that the plan should produce results now, and Target indicates that it should produce results in the future. Specify the expected costs of the treatment plan. Set residual-risk values (which rate the immediate, rather than long-term, impact of the plan): select likelihood and impact models and values. View treatments included within the plan. Or, create or modify them; select Create or Edit options from the Actions menu. (You can also delete a selected treatment.)

If you choose to create or edit a treatment, a page opens for that purpose. In it, specify a name, description, type, and costs. Select one or more controls intended to mitigate risk, and set stratification values for them.

Events and Consequences

Events and consequences apply to you only if, in Administration > Module Management, your company has configured the risk object to include them. If not, prompts to manage or create events and consequences do not appear among the Risk Management tasks in the Navigator.

An event is a set of circumstances under which a risk may manifest itself; it's more narrowly focused that the risk itself. If, for example, the risk states "Earthquake shuts down production at factory," an event might state, "Mild earthquake prompts brief closure for safety inspection." The associated consequence might then enumerate the loss resulting from the brief closure.

To create an event, select the Create Event prompt among the Risk Management tasks. (Or, from the Manage Events page, select Actions > Create.) A Create New Event page opens.

- In its Event Details panel, supply a name and description (which define how the event is an instance of the risk with which it will be associated). Also select a likelihood model and a likelihood value from that model; see "Work with Risk Models." (Impact is expressed by the consequence, and so no impact-model selection is appropriate for the event.)
- In the Consequences panel, select Actions > Add to associate at least one consequence with the event; your selections appear as rows in a grid. (If you have not yet created a consequence for the event, you can do so later, then edit the event to add the consequence.)
- In a Related Risks panel, view the risks to which this event applies. (At least one is specified during risk configuration, and values may appear here only after risks have been edited to include this event.)

To create a consequence, select the Create Consequence prompt among the Risk Management tasks. (Or, from the Manage Consequences page, select Actions > Create.) A Create New Consequence page opens.

- In its Consequence Details panel, supply a name and description (which define how the consequence expresses the impact of an event with which it will be associated). Also select an impact model and an impact value from that model; see "Work with Risk Models." (Likelihood is expressed by the event, and so no likelihood-model selection is appropriate for the consequence.)
- In a Related Events panel, view the events to which this consequence applies. (At least one is specified during event configuration, and values may appear here only after events have been edited to include this consequence.)

To manage either type of object, select the appropriate Manage prompt from the Risk Management tasks. Each lists existing events or consequences, and you can use standard search features to filter the list. You can use a Create option in the Actions menu to create new events or consequences. Or, you can click in the row for an existing event or consequence, then select among Actions options to edit, copy, or delete it. Click on the name of an event or consequence to view its details.

3

Control Management

An EGRCM control documents measures your company takes to address a risk. It describes actions taken externally to EGRCM, either automatically in other systems or manually.

Any number of controls may apply to a given risk; they are associated with the risk when the risk is created or edited. When that occurs, controls are "stratified": they are given values that that define the role each plays in mitigating the risk (see page 3-8). Although stratification formally occurs as you configure a risk, you should bear in mind the role a control will play as you create the control.

For each control, you can create test plans. These document steps to be followed in determining whether the control is effective and whether additional treatment is required.

Creating a Control

To create a control, select Create New Control among the control-management tasks. Or, select Actions > Create (or the create icon) from the Manage Controls page; see page 3-2. A Create New Control page opens.

In this page:

1. Enter mandatory values in the Control Details panel:
   - Enter a name. This should indicate how the control mitigates a risk.
   - Select a method: Manual indicates that the control requires human action. (For example, a manual control might require a person to review an insurance policy before renewal.) Automatic indicates the control is implemented in a system external to EGRCM.
2. Optionally, enter additional values that define the control further:
   - Enter a description. Along with the control name, this should tell how the control mitigates a risk.
   - Select a type. (Values available in the Type LOV are created at the Manage Lookups page, available in the Setup and Administration tasks. If no existing type is appropriate for the control you are creating, you may have a new

type created in the Manage Lookups page. See the *Oracle Enterprise Governance, Risk and Compliance User Guide*.)

- Select an enforcement type, which indicates whether the control corrects a risk, detects its occurrence, or prevents it from occurring.
- Select a frequency with which the control should be implemented.
- Select a currency in which monetary amounts affected by the control are expressed. Also enter an estimate of the cost for implementing the control.
- Select types of assertions the control will evaluate. An assertion is a statement 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 Completeness, Existence or Occurrence, Presentation and Disclosure, Rights and Obligations, and Valuation or Allocation.
- Select check boxes to determine whether the control is in scope for audit testing and assessment.
- Attach files to the control (see page 1-4).
- Set a status for the control — Active or Inactive.
- Type comments, if any are germane.

3. If user-defined attributes have been created for the control object, fields representing these UDAs appear in an Additional Details panel. Provide values for these fields.

4. Optionally, create a test plan. Select the Save button to activate the Test Plans panel. In that panel, select Actions > Create (or the create icon) ; a Create Test Plan page opens. (For instructions on its use, see page 3-3). Having created a plan, click its Save and Close option to return to the Create New Control page.

5. In the Perspectives panel, select perspective values appropriate to the control (see page 1-3).

6. Save or submit the control (see page 1-7).

Managing Controls

From a Manage Controls search page, display a summary list of existing controls. You can create a new control. You can select a control and edit, copy, or delete it. To open the page, click on Manage Control in the Control Management tasks.

From a Manage Controls page specific to a selected control, view or edit control details, or create test plans appropriate for the control. You can also assess the control (page 6-1), create or review an issue against it (page 5-1), or (potentially) review incident results assigned to it (page 1-5). To open the Manage Controls page for a specific control, click on its name in the Manage Controls search page.

Edit, Copy, or Delete Controls

From the Manage Control search page, click in the row for a control. Then do any of the following:

- Edit the control. Select Actions > Edit Control. (Or, select Actions > Edit Definition in the Definition tab of the control-specific Manage Control page.) An Edit Control page opens; it's laid out similarly to the Create Control page, and in general you can modify control values in the same way as you create them. As you edit a control, you can create or modify test plans for them .
- Copy the control, as a template for the creation of a new control. Select Actions > Copy Control, and Create Control page opens, populated with values for the control you've copied. Modify them as you would if you were editing a control.
- Delete the control. Select Actions > Delete Control (or the delete icon). A confirmation message appears; click on its OK button. (A control can be deleted only if its state is New — if it has been saved, but not submitted. If a control cannot be deleted, the Delete Control option is disabled.)

View Control Details

From the Manage Control search page, click on the name of a control to open a management page specific to it.

From the Definition tab of that page, a Control Details section displays the values configured for a control as it was created or edited. You can view or create comments (to do the latter, click the add Comments button). You can view, but not modify, the perspective values assigned to the control, and the risks related to the control.

Test Plans

From the page in which you create or edit a control, you can create test plans for it. A plan consists of a set of "instructions" users follow to verify that the control effectively serves its purpose in mitigating risk; each instruction may comprise any number of "steps." Users execute a test plan while completing an assessment of the control to which the plan is attached.

To create a test plan:

1. In the create page for a control, enter values in the Details panel, then select the Save option to activate the Test Plans panel. In the edit page for a control, the Test Plans panel is active by default. In an active Test Plans panel, select Action > Create (or the create icon). A Create Test Plan page opens.
2. In the Test Plan Details panel:
   - Enter a name and, optionally, a description for the plan.
   - In an Assessment Type field, select the activity type (see page 6-1) for the assessment in which the plan will be executed. In a Test Frequency field, select an interval at which testing should be performed.
   - Optionally, attach files to the plan (see page 1-4).

3. If user-defined attributes have been created for test plans, fields representing these UDAs appear in an Additional Details panel. Provide values for these fields.
4. In a Test Instructions panel, select Actions > Create Manual, or click the Create Manual button. A Create Manual Test Instruction page opens.
5. In its Test Instruction Details panel:
   - Enter a name and, optionally, a description for the instruction.
   - Enter a sample size — a number of control-enforcement instances that must be examined for this instruction to be completed.
   - Optionally, attach files to the instruction.
6. If appropriate, create steps for completing the instruction. In the Test Steps panel, select Actions > Create. A numbered row appears; in it, enter a step description. Repeat this for each of the steps required for the instruction. You can also use options in the Actions menu of the Test Steps panel to delete steps or to rearrange their order.
7. Select Save and Close to Return to the Create Test Plan page. If appropriate for your plan, repeat steps 4–6 to create additional instructions.
8. Select Save or Save and Close.

In the Test Plan Details panel of the Create Test Plan page, a Total Sample Size field displays the sum of the sample-size values you've entered for all test instructions. As users execute the test plan during assessments, EGRCM updates the Samples Collected and Samples Outstanding fields.

4

Base Object Management

A base object is primarily (although not always) the focus of GRC efforts. Within a module, other objects refer, directly or indirectly, to it. For example, the Financial Governance module uses one base object, which is configured as "Process"; it represents business processes for which users identify risks and create controls to mitigate those risks. In each module, the term "base object" is typically renamed to something meaningful (such as "Process" in the Financial Governance module.)

As you work with base objects, you can create "action items" for them. An action item is simply a task you choose to document. It differs from an issue in that it is not necessarily a defect logged against the base object. For example, if you have defined a process for year-end closing, you might require an action item to verify that certain tax documents are included in the year-end reporting.

Creating a Base Object

To create a base object, select the Create option for that object among the base-object-management tasks. (In the Financial Governance module, for instance, this would be Create Process in the Process Management tasks list.) Or, select Actions > Create (or the create icon) in the Manage page for the object.

In the Create page:

1. Enter mandatory values in the Details panel:
    - Compose a name and description. These should define the object. As an example for a process, the name might be Year-End Closing, and the description might be a brief overview of activities required to complete the closing.
    - Select a status (Active or Inactive).
2. Optionally, enter additional values that define the base object further:
    - Select a type. (Values available in the Type LOV are created at the Manage Lookups page, available in the Setup and Administration tasks. If no existing type is appropriate for the base object you are creating, you may have a new type created in the Manage Lookups page. See the *Oracle Enterprise Governance, Risk and Compliance User Guide*.)

- Select check boxes to determine whether the base object is in scope for audit testing and assessment.
- Attach files to the base object (see page 1-4).
- Type comments, if any are germane.

3. If user-defined attributes have been created for the base object, fields representing these UDAs appear in an Additional Details panel. Provide values for these fields.
4. In the Perspectives panel, select perspective values appropriate to the base object (see page 1-3).
5. If, during module setup, the base object was configured so that other objects can be related to it, a Related Object panel appears. In it, select objects (see page 1-4). In the Financial Governance module, for example, you can select risks that may affect a process.
6. Save or submit the base object (see page 1-7).

Managing Base Objects

From a general management page for base objects, you can display a summary list of existing base objects (using standard search features to filter them). You can create a new base object. You can select a base object and edit, copy, or delete it. To open the general management page, click on the Manage option among the base-object management tasks. (In the Financial Governance module, for instance, this would be Manage Process in the Process Management tasks list.)

From a management page specific to a selected base object, you can view and edit its details, or create action items appropriate for the base object. You can also assess the base object (see page 6-1), create or review an issue against it (see page 5-1), or (potentially) review incident results assigned to it (see page 1-5). To open the Manage page for a specific base object, click on its name in the general management page.

Edit, Copy, or Delete Base Objects

From the general management page for base objects, click in the row for a base object. Then do any of the following:

- Edit the base object: Select Actions > Edit, or the edit icon. (Or, select Actions > Edit Definition in the Definition tab of the base-object-specific management page.) An Edit page opens; it's laid out similarly to the Create page, and in general you can modify base-object values in the same way as you create them.
- Copy the base object, as a template for the creation of a new object. Select Actions > Copy (or the copy icon), and Create page opens, populated with values for the base object you've copied. Modify them as you would if you were editing a base object.
- Delete the base object. Select Actions > Delete (or the delete icon). A confirmation message appears; click on its OK button. (A base object can be deleted only if its state is New — if it has been saved, but not submitted. If a base object cannot be deleted, the Delete option is disabled.)

View Base Object Details

From the general management page for base objects, click on the name of an object to open a management page specific to it. From the Definition tab of that page, a Details section displays the values configured for a base object as it was created or edited. You can view or create comments (to do the latter, click the add Comments button). You can view, but not modify, the perspective values assigned to the base object, and objects related to the base object.

Action Items

From the management page specific to a selected base object, you can create action items for the object:

1. Do either of the following:
   - Select the Action Items tab. In an Action Items panel, select Actions > Create (or the creation icon).
   - Select Actions > Create Action Item near the upper right of any tab available in the base-object management page.

   In either case, a Create Action Item page opens (as shown at the top of the next page).
2. Enter required values: A name for the action item and instructions on how to complete it; a start date and a due date; a priority. Also, select a progress value; typically, as you create the action item, select Assigned. As users work to complete the action item, they may select other values — Blocked, Delayed, On Target, or Completed.
3. Optionally, write comments for, or attach files to, the action item. (See page 1-4 for a discussion of file attachment.)

   You can also set a target completion date, although typically this value is set later if a user working to complete the action item determines that actual completion will occur sooner or later than the due date.
4. Select Save or Save and Close.

An action item, once created, appears as a row in the Action Items panel of the Action Items tab. To view its details, click in its row. To alter its progress setting or target completion date, click in its row, select Actions > Edit, and modify values (or add comments) in an Edit Action Item page. (You can instead delete an action item by clicking its row in the Action Items panel and selecting Actions > Delete.) To indicate that the action item is completed, click its row and then click the Mark Complete button.

In the Action Items tab, a Key Performance Indicators panel displays a graph indicating the percentage of action items that have been completed, as well as counts of action items at each of the progress statuses.

5

Issue Management

An issue is a defect or deficiency detected for an object or for an activity being performed against an object, such as an assessment, risk analysis, or risk evaluation. You can create, review, or close an issue either from Issue Management (among the Navigator options available for a module) or from the Issues tab in the Manage page for a specific risk, control, or base object. You may also create an issue against an assessment in the Assessment tab of the Manage page for a specific object; against a risk analysis in the Analysis tab of the Manage Risk page; or against a risk evaluation in the Evaluation tab of the Manage Risk page.

The evaluation of an issue includes these steps: A user creates an issue. A user with proper privileges validates the issue — determines that the issue requires investigation, closes it, or puts it on hold. If the issue is valid, a user with proper permissions then determines whether a remediation plan is required for the issue to be resolved. (If not, the issue is closed.) If so, a remediation plan is created or selected, users respond to worklists to complete remediation tasks, the remediation plan is marked as complete, and the issue is closed.

Creating an Issue

An issue created from the Manage page for an object is automatically associated with that object:

1. From any tab within a Manage page, select Actions > Create Issue. Or, where appropriate, click a Create Issue button for a particular element of a page (for example, the Risk Analysis grid on the Analysis tab of the Manage Risk page).

   Or, click on the Issues tab and, in the Issue panel select Actions > Create (or the create icon).

2. A Create Issue pop-up window opens. (It's shown at the top of the next page.) Enter a name and description, which define the defect or deficiency the issue is meant to address.

3. Select a severity. (Values available in the Severity LOV are created at the Manage Lookups page, available in the Setup and Administration tasks. If no existing severity is appropriate for the issue you are creating, you may have a new severity value created in the Manage Lookups page.)

4. Optionally, enter values that define the issue more fully: a type (also defined in the Manage Lookups page), and comments.
5. Optionally, attach files to the issue (see page 1-4).
6. Click the Submit button.

From Issue Management, you also need to select the object to which the issue pertains:

1. From the Issue Management tasks, select Create New Issue.
2. In an Issue Details panel, in addition to the values you would enter if you were creating the issue from the Manage page for an object, select a status — typically, as you create an issue, Open. (Other options include On Hold and In Remediation.)
3. Select the object (or objects) against which the issue is being raised. In a Related Objects panel, select Actions > Add; a Related Objects for Issue pop-up window opens. In it, select the type of object you want in an Object Name list box. Use standard search features to filter for the object you want, then click on it in a grid displaying search results. Click the OK button.

   You can also delete objects from the Related Objects panel. Click on the object you want to delete, and select Actions > Remove.
4. Save or submit the issue (see page 1-7).

Managing Issues

From a general Manage Issues page, you can display a summary list of existing issues (using standard search features to filter them). You can create a new issue. You can select an issue for editing, deletion, or closure. To open the general Manage Issues page, click on Manage Issues in the Issue Management tasks.

From a Manage Issue page specific to a selected issue, you can view or edit details about the selected issue. You can also close the issue. Open the issue-specific Manage page in either of two ways:

- From the Manage page for a base object, risk, or control, click on the Issues tab. An Issues panel displays two lists of issues raised against the object — open and closed. Click on the name of the issue you want (although the link is active only if your roles grant access to the issue).

  (Instead, you can click on the row for the issue in the object Manage page. In that case, the object Manage page remains open, and a read-only display of issue details appears.)
- Open the general Manage Issues page. Search for the issue you want and, in its row in a Search Results grid, click on the name of the issue.

Viewing Issue Details

The Manage Issue page for a specific issue displays not only details set as the issue was created, but also details that can be set only as the issue is edited. The latter relate to whether the issue is validated and whether one or more remediation plans are assigned to it.

In a Definition tab:

- A Progress panel displays graphs charting the progress of issue resolution.
- A Details panel shows the values set as the issue was created; impact and remediation costs, an estimate of how likely the incident is to recur, and whether the incident requires remediation (all of which are set as the issue is edited); and information about who has created and updated the incident, and when.
- A Comments panel displays comments (if any) created for the issue.
- A Related Information tab lists the objects against which the issue has been raised.

In a Remediation tab, a grid lists the remediation plans (if any) assigned to the issue.

Editing or Deleting Issues

Regardless of whether you are validating an issue or determining whether it requires remediation, you work in an Edit Issue page specific to a selected issue.

When an issue is created, worklists to the Edit page are issued to users with roles that include validation privileges. Such a user may close issue if he deems it invalid, resubmit it at the Open status if he deems it valid, or place it at an On Hold status.

Once the issue is validated, worklists leading to the Edit page are issued to users with roles containing issue management privileges. Such a user may set details pertaining to remediation, add to objects against which the issue is raised, and select remediation plans.

In practice — for a user with appropriate privileges — these two steps may be combined into one.

Apart from responding to worklists, you can open the Edit Issue page in either of two ways:

- From the general Manage Issues page, enter search parameters to locate the issue you want, and then click in its row the Search Results panel. Then select Actions > Edit (or the edit icon).
- From the Manage page for a specific issue, select Actions > Edit Issue. (The Actions menu is near the upper right corner of the page.)

As you edit an issue, you can use an Issue Details panel to modify any of the values set as the issue was created. You can also associate the issue with objects other than the one for which it was created. You can also set these values:

- Likelihood of Recurrence: Values available in this LOV are created at the Manage Lookups page, available in the Setup and Administration tasks. If no existing likelihood is appropriate for the issue, you may have a new likelihood value created in the Manage Lookups page.
- Requires Remediation: Select Yes or No.
- Currency: Select the currency in which issue impact and remediation costs are measured.

- Impact: Enter a range of monetary values to estimate what costs the issue would cause if left untreated.
- Remediation Cost: Enter a range of monetary values to estimate the cost of acting to resolve the issue.
- Source: Select Internal or External to indicate whether the issue was brought to light by a person inside or outside of your organization.

In a Remediation Plans panel, do any of the following:

- Select a remediation plan for the issue: Click on the green plus sign. A Search: Remediation Plan pop-up window opens. Enter search parameters to locate the plan you want, click on its row in a grid, and click the Done button.
- Create a new remediation plan for the issue: Click on the create icon and respond to a message indicating that changes to the issue will be saved. The Create Remediation Plan page then opens (see page 5-5).
- You can also select a plan and edit it (use the pencil icon) or delete it (use the red × icon).

In the Comments panel, click the Add Comments button; and Add Comments pop-up window opens. Type a comment in it and click its OK button. The comment then appears in the Comments panel.

You can delete an issue only from the general Manage Issues page (and only if the issue's state permits deletion). Select the issue in the Search Results grid on that page, then select Actions > Delete.

Closing Issues

An issue may be closed if a user with appropriate permissions determines that it is not valid, that it does not require a remediation plan, or that remediation is complete. (A user may also close an issue if it duplicates another issue or if it cannot be resolved.)

To close an issue, do any of the following:

- From the general Manage Issues page, click in the row representing an issue, and then select Actions > Close (or click the Close button).
- From the Manage Issue page specific to a selected issue, select Actions > Close Issue.
- From the Edit Issue page, click on the Close Issue button.

In each case, a Close Issue pop-up window opens. Select a reason for closing the issue in a "Specify the Reason for this action" list box. (Values available in this LOV are created at the Manage Lookups page, available in the Setup and Administration tasks. If no existing reason is appropriate for the issue you are closing, you may have a new reason created in the Manage Lookups page.) Optionally, add comments in the Comments field, and click on the OK button.

Remediation Plans

A remediation plan consists of tasks that users complete to investigate and resolve an issue. For example, an issue may have been created because a test plan for a control contained no instructions, causing an assessment to fail. The remediation plan would be to correct the control test plan definition, and its tasks might include, first, to determine the steps needed to test the control and, second, to update the test plan instructions. Users with appropriate roles receive worklists to complete the plan.

To create a remediation plan, select Create Remediation Plan among the Issue Management tasks. (Or, from the Manage Remediation Plans page, select Actions > Create.) A Create Remediation Plan page opens.

In this page:

- In the Remediation Plan Details panel, supply mandatory values. These include a name and description (which summarize how the plan will address its issue). Also these include priority, due date, progress (typically, when the plan is created, this value is On Target), and status (typically, when the plan is created, this value is Active). Users will update the progress and status values as they complete the plan.
- In the Remediation Plan Details panel, optionally supply other values that define the plan further. These may include an estimated date (although typically this value is set later if a user working to complete the plan determines that actual completion will occur sooner or later than the due date), attachments (see page 1-4), and comments.
- Select the Save button to activate the Remediation Tasks panel. In that panel, select Actions > Create (or the create icon) to open a Create Task page. Mandatory values include name, start date, priority, status (select Active as you create the task), and description (which tells what a user must do to complete the task). Optional values include due date; estimated date and progress code (again, typically supplied by users as they complete the task); and attachments and comments.

  In the Create Task page, select Save and Close to return to the Create Remediation Plan page. In its Remediation Tasks panel, you can select Actions > Create (or the create icon) to create an additional task. Or you can select an existing task and select Actions > Edit (or the edit icon) to modify it, or Actions > Delete (or the delete icon) to remove it.

To work with a remediation plan, you can respond to worklists concerning the plan. Or, select Manage Remediation Plans from the Issue Management tasks; a Manage Remediation Plans page opens, in which you can use standard search features to filter a list of existing plans. Click on a plan name to view its details, and from the view page select Actions > Edit Definition (or the edit icon) to modify those details. Or, to reach the edit page directly from the Manage Remediation Plans page, click in its row and select Actions > Edit.

As you work to complete a task, update its progress code — it may remain on target, or be blocked or delayed. In the event of blockage or delay, update the estimated date as well. When the task is done, update its status to Completed. Add comments that explain the actions you're taking or reasons for delay.

As you work to complete the remediation plan, update its progress and status. Once again, progress values include On Target, Blocked, and Delayed. Select a status that reflects the progress; for example, On Hold if progress is blocked, or Completed if progress is On Target and you have finished work on the remediation plan. Again, add comments to explain the current status of the plan.

6

Assessment Management

An assessment is the review of a base object, risk, or control, initially to ensure that it is defined correctly, and subsequently to ensure that its definition remains appropriate. An assessment might be "ad hoc" (initiated from the page on which an object is created) or initiated through the Assessment Management page.

No matter whether an assessment is ad hoc or initiated through Assessment Management, it specifies an activity type, which determines what the assessment is meant to uncover. Types can include the following:

- Certification — Is the information in this assessment of an object accurate and complete?
- Assess Risk — Is a risk appropriately documented, is its analysis current, is its evaluation accurate, and are treatments active?
- Audit Test — Does a risk, control, or base object meet audit guidelines?
- Operational Assessment — Does a control or base object operate effectively and as designed?
- Design Review — Is a base object or control designed effectively and does it meet its guidelines?
- Documentation Update — Does a base object have required documentation?

Preparing Templates and Plans

If initiated through Assessment Management, an assessment is based on a plan, which is in turn developed from a template. (An ad hoc assessment does not require a plan or template.) Select Assessment Management from the Tools options in the Navigator.

Assessment Templates

As you create an assessment template, you name it and select the following values:

- Which module is to be assessed.
- A "primary object" of assessment: For a module, this may be base object ("Process" for Financial Governance), control, or risk.

- An "assessment type," for which values are maintained in the Manage Lookups page. (If no existing type is appropriate for the template you are creating, have a new type created in the Manage Lookups page. See the *Oracle Enterprise Governance, Risk and Compliance User Guide*.)
- One or more activity types (see page 6-1).

To view or edit templates, use features available from the Manage Templates link among the Assessment Management tasks. To create a template, select Create Template.

Assessment Plans

As you create an assessment plan, you name it and select a template for it. A Template Activities grid then displays a row for each activity type configured for the template. (Each row also displays the primary object selected for the template, in a column labeled Business Entity Type.)

You may wish to have users answer specific questions as they complete assessments, and if so you will have created surveys containing those questions. (See chapter 7.) Each survey is based on a template of its own. As you create an assessment plan, you may use the Template Activities grid to select one survey template for each assessment activity: Select an activity (row) in the grid and click the Edit icon (which looks like a pencil). An Edit Survey Template pop-up window opens; in it, select the survey template you want.

In the assessment plan, you may also add "selection criteria," "perspective selection criteria," or "additional criteria" — filters that narrow the focus of any assessment initiated from the plan. If the primary object of the assessment is control, for example, you may filter controls by name, or select controls associated with a given perspective value, or select controls with particular stratification values, among other options.

However, you may choose not to set any criteria. This would increase the flexibility of the plan, because users would be able to specify distinct sets of criteria as they use the plan to initiate assessments.

To view or edit existing plans, use features available from the Manage Plans link among the Assessment Management tasks. To create a plan, select Create Plan.

Initiating an Assessment

You may initiate an assessment from within Assessment Management:

1. Select Initiate Assessment from the Assessment Management tasks.
2. In a General page, enter a name and description for the assessment, select an assessment plan, and set start and due dates.

   If you select a plan in which any activity is associated with a survey template, a Survey Name Prefix field becomes not only active, but also mandatory. In it, enter any value you choose, up to 150 characters. (The prefix is used to give the survey a unique name.) If the assessment plan does not specify a survey, the Survey Name Prefix field remains disabled.

   When you finish working in the General page, click the Next button.

3. In a Selection Criteria page, optionally choose selection, perspective, or additional criteria from among those made available by the plan you selected in step 2. Fields in this page look like those in the Create Assessment Plan page. Then click the Next button.
4. In a Components page, select Actions > Generate to produce a list of the objects made available by the plan you selected in step 2 and any criteria you specified in step 3. Ensure that the Include check box is selected for those objects you want to include in the assessment, and cleared for those you do not. (You can select any number of objects from the list you've generated.) When you finish selecting objects, click on the Next button.
5. In a Participants page, review users who are to complete the assessment. (These users are selected automatically; the selection is determined by their roles. You cannot change anything on this page.)
6. Select Save or Submit.

Alternatively, you may initiate an ad hoc assessment for a base object, risk, or control you want to assess:

1. Navigate to the Manage page specific to an individual base object, risk, or control.
2. Click on its Assessment tab, and then on Actions > Create Assessment.
3. A Create Assessment pop-up window opens. In it:
   - Select an activity type, which determines what the assessment is meant to uncover. Types are listed on page 6-1, although you will see only those appropriate for the object you are assessing.
   - Compose a name and description for the assessment, and select start and due dates.
4. Select the Create button.

Completing an Assessment

When an assessment is initiated from Assessment Management, any number of objects may be selected to be assessed. Each of these objects is assessed individually. (An ad hoc assessment necessarily concerns the individual object from which it is initiated.) Assessors may:

- Select a worklist entry for an object included in the assessment.
- Among the Assessment Management tasks, select Complete Assessment. In a My Assessments page, search for the assessment and select the record for one of the objects included in the assessment.
- From the Assessments tab of the object being assessed, select the assessment, then click the Complete or Review/Approve button (depending on the user's role and the status of the assessment).

Depending on the object being assessed, assessors are presented with some or all of the following screens:

- An Introduction screen presents an overview of the object being assessed. Any attachments associated with the assessment are available here also.

- A Prior Results screen displays results from prior assessments. The state of assessments can be New, In Review, Awaiting Approval, Rejected, or Complete.
- If a control with a test plan is being assessed, an Enter Results screen enables the assessor to complete the test plan.
- If a survey is attached to the assessment, the assessor can complete it in the Survey screen.
- On the Complete Assessment page, a assessor may enter results of the assessment, create an issue, or attach a file to the assessment.

The following result options are seeded in the application. An administrator can modify the names of the result options (via the Setup and Administration > Manage Assessment Results), 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.

Canceling Assessments

When an assessment is initiated in Assessment Management, you may determine that one of the objects selected for assessment should not have been included. If so, you can cancel its assessment, while allowing the assessment of all the others to proceed. For you to do so, the assessment for that object must be in the New, In Edit, or Rejected state. (This cancellation feature does not apply to ad hoc assessments.)

To cancel the assessment of an object:

1. Among the Assessment Management tasks, select Manage Assessments.
2. In the Manage Assessments page, click on the name of the assessment from which you want to remove an object.
3. A Manage Assessments Details page opens. In its Components panel, select the object you want to remove.
4. Click the Cancel Assessment button, and select Yes in a Cancel Assessment confirmation pop-up.

   If the assessment for this object had been in New, In Edit, or Rejected state, the state changes to Canceled. If the assessment had been in any other state, an error message states that the assessment cannot be canceled.

Managing Assessment Results

In a Manage Assessment Results page, an administrator can edit responses from which users can select as they perform assessments. To open this page, select Setup and Administration from the Tools options in the Navigator. Then select Manage Assessment Results in a Setup list of tasks.

In the Manage Assessment Result page, locate the response you want to edit, and modify its Response Name value. Then click the Save button. You cannot modify response codes. You cannot add new responses or delete existing responses.

7

Survey Management

You can create surveys to assist in evidence gathering for assessments and other testing. You can also create general surveys unrelated to assessments or testing. A survey may include any type of question.

To work with surveys, select Survey Management among the Tools tasks available in the GRC Navigator.

A survey is based on a template, which incorporates the questions to be asked. While creating a template, you can formulate questions for it, or select questions that have been prepared in advance. For each question, you select a format (such as multiple choice); depending on the format, you may provide answers from which responders can choose — either create "question choices" (possible answers) or select a "choice set" (an already-created set of answers).

Survey questions may take the following formats:

- Single response: Radio buttons present multiple options from which a responder can select only one.
- Single response with other: Like single response, except one option is Other, for which the responder can enter a text value.
- Single response drop down list: A list of value presents multiple options, from which a responder can select only one.
- Multiple choice list box: A scrolling list box presents multiple options, from which a responder can select any number.
- Check all that apply: Check boxes present multiple options, from which a responder can select any number.
- Check all that apply with other: Check boxes present multiple options, from which a responder can select any number. One option is Other, for which the responder can enter a text value.
- Rating on scale: Radio buttons present a range of values; a responder can select only one.
- Numeric allocation: A responder enters a number for each of several options, quantifying each in comparison with the others.
- Open text: A text box enables responders to enter free-form text.

Before you initiate a survey, ensure that the components you need are ready: You may, for example, create choice sets for inclusion in questions, create questions for inclusion in a template, create the template, and then initiate the survey. If your questions don't require choice sets, you may start at the question-creation step. You may start at the template-creation step, and simply create questions from within the template. Or, you may initiate a survey from an existing template.

Survey Choice Sets

For a choice set, select from available choices (possible answers to questions) or create new choices, manipulate the order in which they will appear, and select a question format to which they apply. To view or edit existing choice sets, select Manage Survey Choice Sets from the Survey Management tasks. Select Actions > Create to produce a new choice set. Click on a choice set and select Actions > Edit to modify it, Actions > Duplicate to copy it (as a source for a new choice set), or Actions > Delete to remove it.

Survey Questions

For a survey question, enter details — a type, the question itself (the text that will be presented to responders), and a status. Also select its format. If appropriate, select a choice set (a field appears for this purpose if you choose a format that requires choices) or create question choices and arrange the order in which they will appear. (If you create choices, you can also save them as a choice set.)

To view or edit questions, select Manage Survey Questions from the Survey Management tasks. Select Actions > Create to produce a new question. Click on a question and select Actions > Edit to modify it, or Actions > Copy to use it as a source for a new question. (Alternatively, create questions from within Manage Survey Templates.)

Survey Templates

For a survey template, select a type and status, then enter "survey content": compose instructions for completing the survey, select or create questions (the create-question functionality here is the same as it was in Manage Survey Questions), and arrange the order in which they will appear. If GRC is configured to make more than one language available to users, you can also select languages into which surveys must be translated.

To view or edit templates, select Manage Survey Templates from the Survey Management tasks to open a Manage Survey Templates page. Select Actions > Create to produce a new template. Click on a template and select Actions > Edit to modify it, or Actions > Copy to use it as a source for a new template. From the Manage Survey Templates page, you can also select a template and use it to initiate a survey.

Initiating Surveys

Finally, to initiate surveys, select the template you want to use for the survey, select an end date, choose both the type and actual instance of a component (such as control or risk) about which the survey will ask questions, and select people who must respond to the survey. To do so, select Manage Surveys from the Survey Management tasks, then click on the row representing a template and select Actions > Create. (Alternatively, from Manage Survey Templates, select a template and click an Initiate Survey button.) From Manage Surveys, you can also select a survey and edit it (add responders) or view responses to it.

Completing Surveys

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.