Oracle® Enterprise Governance, Risk and Compliance Manager

User's Guide

Release 1

Part No. E15287-01

September 2009

ORACLE

Oracle Enterprise Governance, Risk and Compliance Manager User's Guide, Release 1

Part No. E15287-01

Primary Author: Denise Fairbanks Simpson

Contents

Send Us Your Comments

Oracle Enterprise Governance, Risk and Compliance Manager User's Guide, Release 1

Part No. E15287-01

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

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

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

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

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

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

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

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

Preface

Intended Audience

Welcome to Release 1 of the *Oracle Enterprise Governance, Risk and Compliance Manager User's Guide.*

This guide is primarily intended for people who create and manage business processes that support financial compliance, contribute information to processes, and create and resolve issues regarding processes. It is also intended for management and for auditors who monitor, evaluate, and report business process activity against financial compliance processes.

See Related Information Sources on page x for more Oracle Applications product information.

Deaf/Hard of Hearing Access to Oracle Support Services

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

Documentation Accessibility

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

technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at http://www.oracle.com/accessibility/.

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

Structure

Related Information Sources

Oracle Enterprise Governance, Risk and Compliance Manager Implementation Guide

Do Not Use Database Tools to Modify Oracle Applications Data

Oracle STRONGLY RECOMMENDS that you never use SQL*Plus, Oracle Data Browser, database triggers, or any other tool to modify Oracle Applications data unless otherwise instructed.

Oracle provides powerful tools you can use to create, store, change, retrieve, and maintain information in an Oracle database. But if you use Oracle tools such as SQL*Plus to modify Oracle Applications data, you risk destroying the integrity of your data and you lose the ability to audit changes to your data.

Because Oracle Applications tables are interrelated, any change you make using an Oracle Applications form can update many tables at once. But when you modify Oracle Applications data using anything other than Oracle Applications, you may change a

row in one table without making corresponding changes in related tables. If your tables get out of synchronization with each other, you risk retrieving erroneous information and you risk unpredictable results throughout Oracle Applications.

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

1

About Enterprise Governance, Risk and Compliance Manager

What is Governance, Risk and Compliance?

Worldwide, legislators, regulators and investors are placing increasing mandates on businesses to improve transparency and controls over financial and compliance reporting. Laws such as the U.S. Sarbanes Oxley Act, Canadian Bill 198, OMB Circular 123A, and Japanese SOX (J-SOX), are forcing organizations to adopt rigorous approaches to documenting and testing internal processes and controls. Oracle's Enterprise Governance, Risk and Compliance Manager provides the solution to these requirements.

Enterprise Governance, Risk and Compliance Explained

Enterprise Governance, Risk and Compliance Manager (EGRCM) helps reduce the cost and complexity of compliance and help leverage compliance efforts to create new process efficiencies. A set of self-contained, loosely coupled functional modules called Application Modules collectively provide an integrated system of components necessary to manage Governance, Risk, and Compliance objectives. Application modules in EGRCM include a GRC Framework Application Module and a Financial Governance Module.

GRC Framework Explained

Business initiatives are documented processes that include metrics and time frames and are used to define business goals. The GRC Framework is the foundation that provides core services and application business components (that is, the building blocks), from which all business initiative specific application modules are built.

All GRC business initiatives share common building blocks that are defined by industry standard frameworks such as COSO, COBIT, ITIL, and ISO. GRC Framework provides

the basic building blocks necessary to create a Fusion GRC Manager Application Module to suit the requirements of any GRC business initiative.

Components Explained

Components are reusable, fundamental building blocks that describe common core objects such as risks or controls. There are also GRC Components, which are general purpose objects that can be defined as needed. For example, you can create a GRC Component for business process. When included in a business model, components are used to support a specific GRC initiative, such as financial compliance.

- Component Types can be user defined
- Components can be extended using user defined attributes
- Changes to components are tracked through revisions and versioning

What are User Defined Component Types (UDT)?

User defined component types (UDTs) are additional business components that you can create as necessary to complete the requirements for any GRC business initiative. You can create UDTs for the following core component types:

- Risks
- Proposed risks
- Events
- Consequences
- Controls
- GRC Components
- Issues
- Remediation plans
- Perspective items

What are user defined attributes?

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

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

Refer to the Governance, Risk and Compliance - Fusion Edition Implementation Guide for details on creating UDAs.

Perspectives Explained

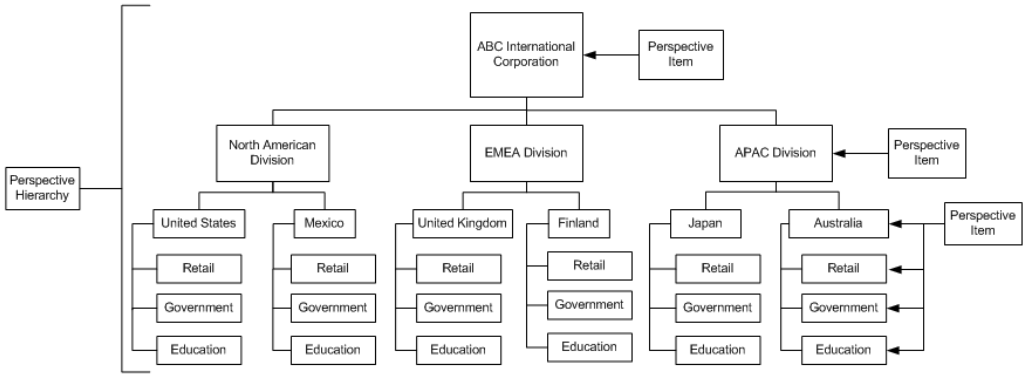
Perspectives provide hierarchical shape, structure and organization for core business components such as risks, controls and GRC components. They also support key user activities such as analytics and reporting. Perspective management provides a centralized interface for users to define different views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

Perspectives contain the following elements:

- Perspective items: The element that is associated to a component.
- A perspective hierarchy: The structure or arraignment of the perspective items.

The perspective hierarchy contains the structure and the relationships between the perspective items with references to the perspective items themselves. This enables perspective items to be in multiple hierarchies.

The following is an example of a corporate structure hierarchy:



For additional information, refer to Managing Perspectives, page 3-1.

Organization Perspective Explained

Organization is a delivered perspective type that has additional features that are not available to other perspective types. The relationship to the organization perspective item is propagated down to the other related business components. The business component within the information model that will be the focal point for the

organization propagation is defined in the module configuration.

For example, in the Financial Governance module, business process objects must have an associated Organization perspective. You define the organization for the process and then, when a risk is related to the process, the organization perspective of that process becomes the organization perspective for the risk. Likewise, when a control is related to the risk, the control receives the organization perspective from the risk.

Are perspectives required?

Whether or not a perspective is required is defined during object configuration.

What is a Risk?

A risk is defined as the chance of an event occurring that will have a positive or negative impact on the objectives of the organization or a division.

What is an Event?

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

What is a Consequence?

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

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

What is a Control?

A control is an existing process, policy, device, practice or other action that acts to minimize negative risk or enhance positive opportunities.

Issues Explained

Issues are reported defects or deficiencies against any component or its related components such as risks, controls, or GRC Components such as business processes. Issues:

- Can be associated with any component (risk, control, GRC Component)
- Are assigned to other users for validation and disposition which may require

remediation

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

What is remediation?

Remediation is the process of correcting or addressing an issue.

What is a remediation plan?

A remediation plan is the documented response actions for an issue and is the way progress on the resolution of the issue is tracked.

Assessments Explained

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

Surveys Explained

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

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

Application Modules Explained

An application module is a collection of user defined component types (for example, Financial Compliance Risk, Financial Compliance Controls, Financial Compliance Process) that is configured to depict the underlying information model of the GRC solution, such as a financial compliance model. Application modules:

- Identify the set of component types that are necessary to solve a specific GRC business initiative (for example, process, risk, and control component types that are necessary to address a financial compliance initiative.)

- Define the process flows required for the application module to enable the specific GRC Business Initiatives
- Can be pre-populated with content specific to the business initiative.

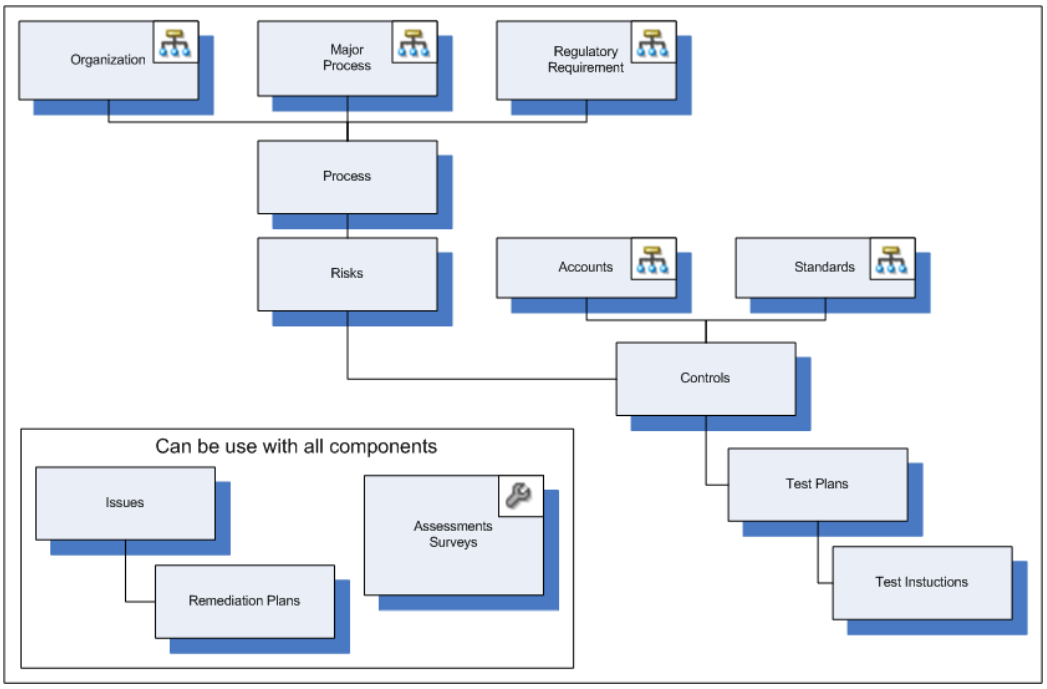
The components that are available for use in an application module are dependent on the component configuration. Components are configured to identify which options are appropriate for a specific module. Refer to the Enterprise Governance, Risk and Compliance Manager Implementation Guide for information on configuration.

What is the Financial Governance Module?

The Financial Governance module is a delivered module that is used to address financial reporting mandates. It includes the following component types:

- Financial Governance Process
- Financial Governance Risk
- Financial Governance Control
- Financial Governance Issue
- Financial Governance Remediation Plan
- Financial Governance Event
- Financial Governance Consequence

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


Organization
Major Process
Regulatory Requirement
Process
Risks
Accounts
Standards
Controls
Test Plans
Test Instuctions
Can be use with all components
Issues
Remediation Plans
Assessments Surveys

2

Basic Application Operation and Common Tasks

Security Overview

User accounts, IDs, and passwords are set up by the GRC Administrator. The GRC Administrator also assigns one or more roles to each user based on their need to work with content and to track activity for compliance.

Users are required to provide a user ID and password to log in to the application. The security allows users to access only assigned functions and content. Functions that a user is not authorized to access do not appear in the interface for a user's account.

Roles Explained

All users are assigned specific roles that allow them to perform only those tasks that are appropriate to their job. This provides security as only users that are assigned certain roles are allowed to perform certain tasks and to access certain data. Administrators can create roles and users as needed. Refer to the EGRCM Implementation Guide for additional details.

Summary of Roles

The following roles are seeded in EGRCM.

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

This role/job role code	Has access to this functionality...
…	

GRC User GRC_User_Job_Role	• Propose a Risk • Complete a Survey
GRC Administrator GRC_Administrator_Job_Role	• GRC Reporting • GRC Analysis • GRC Setup Administration and Configuration
CXO CXO_Job_Role	• Propose a Risk • Complete a Survey • Assessments • GRC Reporting • GRC Analysis • User Access to Control Management • User Access to Risk Management • User Access to Issue Management • User Access to Perspective Management • User Access to GRC Component Management

Risk Administrator Risk_Administrator_Job_Role	• Propose a Risk • Complete a Survey • Assessments • GRC Reporting • GRC Analysis • Administrator Access to Risk Management • Administrator Access to Issue Management • Administrator Access to Perspective Management • Administrator Access to GRC Component Management • Administrator Access to Assessment Management • Administrator Access to Survey Management
Risk Manager Risk_Manager_Job_Role	• Propose a Risk • Complete a Survey • Assessments • GRC Reporting • GRC Analysis • Manager Access to Risk Management • Manager Access to Issue Management • Manager Access to Perspective Management • Manager Access to GRC Component Management • Administrator Access to Assessment Management • Administrator Access to Survey Management

Risk User Risk_User_Job_Role	• Propose a Risk • Complete a Survey • Assessments • GRC Reporting • GRC Analysis • User Access to Risk Management • User Access to Issue Management
IT Controls Manager IT_Controls_Manager_Job_Role	• Propose a Risk • Complete a Survey • Assessments • GRC Reporting • GRC Analysis • Manager Access to Control Management • Manager Access to Issue Management • Manager Access to Perspective Management • Manager Access to GRC Component Management • Administrator Access to Assessment Management • Administrator Access to Survey Management

Internal Controls Administrator Internal_Controls_Administrator_Job_Role	• Propose a Risk • Complete a Survey • Assessments • GRC Reporting • GRC Analysis • Administrator Access to Control Management • Administrator Access to Issue Management • Administrator Access to Perspective Management • Administrator Access to GRC Component Management • Administrator Access to Assessment Management • Administrator Access to Survey Management
Internal Controls Manager Internal_Controls_Manager_Job_Role	• Propose a Risk • Complete a Survey • Assessments • GRC Reporting • GRC Analysis • Manager Access to Control Management • Manager Access to Issue Management • Manager Access to Perspective Management • Manager Access to GRC Component Management • Administrator Access to Assessment Management • Administrator Access to Survey Management

Internal Controls User Internal_Controls_User_Job_Role	• Propose a Risk • Complete a Survey • Assessments • GRC Reporting • GRC Analysis • User Access to Control Management • User Access to Issue Management
Line of Business Manager Line_of_Business_Manager_Job_Role	• Propose a Risk • Complete a Survey • Assessments • GRC Reporting • GRC Analysis • User Access to Issue Management • User Access to Perspective Management • User Access to GRC Component Management

Process Administrator Process_Administrator_Job_Role	• Propose a Risk • Complete a Survey • Complete an Assessment • GRC Reporting • GRC Analysis • Administrator Access to Control Management • Administrator Access to Issue Management • Administrator Access to Perspective Management • Administrator Access to GRC Component Management • Administrator Access to Assessment Management • Administrator Access to Survey Management
Process Manager Process_Manager_Job_Role	• Propose a Risk • Complete a Survey • Assessments • GRC Reporting • GRC Analysis • User Access to Issue Management • Manager Access to GRC Component Management • Administrator Access to Survey Management

Process User Process_User_Job_Role	• Propose a Risk • Complete a Survey • Assessments • GRC Reporting • GRC Analysis • User Access to Issue Management • User Access to GRC Component Management
Issue Administrator Issue_Administrator_Job_Role	• Propose a Risk • Complete a Survey • Assessments • GRC Reporting • GRC Analysis • Administrator Access to Issue Management
Issue Manager Issue_Manager_Job_Role	• Propose a Risk • Complete a Survey • Assessments • GRC Reporting • GRC Analysis • Manager Access to Issue Management

Perspective Administrator Perspective_Administrator_Job_Role	• Propose a Risk • Complete a Survey • Assessments • GRC Reporting • GRC Analysis • Administrator Access to Perspective Management
Perspective Manager Perspective_Manager_Job_Role	• Propose a Risk • Complete a Survey • Assessments • GRC Reporting • GRC Analysis • Manager Access to Perspective Management
Assessment Administrator Assessment_Administrator_Job_Role	• Propose a Risk • Complete a Survey • Assessments • GRC Reporting • GRC Analysis • Administrator Access to Assessment Management within GRC Tools

Assessment Manager Assessment_Manager_Job_Role	• Propose a Risk • Complete a Survey • Assessments • GRC Reporting • GRC Analysis • Manager Access to Assessment Management within GRC Tools
External Auditor External_Auditor_Job_Role	• Propose a Risk • GRC Reporting
Internal Audit Administrator Internal_Audit_Administrator_Job_Role	• Propose a Risk • Complete a Survey • Assessments • GRC Reporting • GRC Analysis • Administrator Access to Control Management • Administrator Access to Issue Management • Administrator Access to Perspective Management • Administrator Access to GRC Component Management • Administrator Access to Assessment Management • Administrator Access to Survey Management

Internal Audit Manager Internal_Audit_Manager_Job_Role	• Propose a Risk • Complete a Survey • Assessments • GRC Reporting • GRC Analysis • Manager Access to Control Management • Manager Access to Issue Management • Manager Access to Perspective Management • Manager Access to GRC Component Management • Administrator Access to Assessment Management • Administrator Access to Survey Management
Internal Auditor Internal_Auditor_Job_Role	• Propose a Risk • Complete a Survey • Assessments • GRC Reporting • GRC Analysis • User Access to Control Management • User Access to Issue Management

Survey Administrator Survey_Administrator_Job_Role	• Propose a Risk • Complete a Survey • Assessments • GRC Reporting • GRC Analysis • Administrator Access to Survey Management within GRC Tools
Survey Manager Survey_Manager_Job_Role	• Propose a Risk • Complete a Survey • Assessments • GRC Reporting • GRC Analysis • Manager Access to Survey Management within GRC Tools

Basic User Interface

What you see on your dashboards is determined by a few factors:

- The roles that are assigned to you
- The module that you are currently in

In addition, your GRC Administrator can configure the system to hide functions that are not relevant to your business process.

Dashboards Explained

There are three types of dashboards that you will see:

- Home Page, or Home Dashboard, is your default landing page that shows your worklist, watchlist and notifications.
- Transaction Dashboards are core to one or more business processes and provide centralized launching pads into key tasks and work areas. They also provide a way

to monitor the status of the underlying transactions.

- Business Intelligence (BI) Dashboards are complementary to the business process. They answer fundamental questions about the health of the business — financial, operational, or comparative in nature. Although transaction dashboards can contain analytics, BI Dashboards contain additional intelligence, analytics and configuration.

Home Page Structure

The home page displays information about your current work. Depending on your role, you may or may not have access all regions. All roles, however can see:

- **Role Selector:** Select a role to limit the view on the Home page to only those objects applicable to the selected role. You will only see roles to which you are currently assigned. Note that the role selection is only valid for the home page; on all other pages, you will see all appropriate documents, regardless of the role you selected on the home page.

- **My Watchlist:** The watchlist is a categorized summary of your work list entries. Within the categories, they are summarized and grouped by activity type. When you select a certain watch list grouping, the appropriate work area for that category is displayed, and only that group of watch list items are displayed within the work list. This narrows down your pending work and brings into focus the work you have selected.

Common Regions on Overview Pages

Most Overview pages contain the following regions:

- **Pending Activities:** Displays:
  - **Worklists:**Displays worklist entries that are assigned to you for the current work area. For example, if you are in the GRC Tools area, you will see your worklist entries for Assessments and Surveys.
  - **Notifications:**Displays a list of notifications of changes (including reviews and approvals) that have been made to objects that are related to objects that you own. For example, if you are the owner of Risk ABC and it is related to Control X, when Control X changes and that change is approved, you are notified that it has changed. You would also get a notification if Risk ABC is analyzed or evaluated.

- **Objects listing:** Displays active objects to which you have access to, and to which you are assigned responsibility via delegation. Refer to Delegation Explained, page 2-18 for additional information. Click on an object to view it.

- **Tasks:** List all tasks that you can perform from the current page.
- **Search:** Depending on the page you are on, you can search by Name, Description, ID, Class, Status, Method, or run a previously saved search.
- **Favorites:**Displays frequently used objects that you have designates as your favorites.

Common Elements in Overview, Dashboard and Component Pages

Common elements in dashboards include:

Element	Description
Linked object names	Enable you to perform management tasks for objects that are delegated to you
Bars or pie slices in graphs	Mouse over to view details for that slice or bar, or click to drill to secondary pages that provide additional details.
Filters	Enable you to limit the data that you are viewing in the current chart or graph. In many table you can filter by date or status
Date slider	Enables you to modify the date range displayed in the current chart

Action Icons	Shortcuts that enable you to perform actions.

	Creates a new object
	Edit the current object
	On overview pages, use to delete the object. In regions where an object is referenced, such as Related Controls or Delegates, use to remove the selected object from the current field. This does not delete the object, it just removes the association with the current object
	The regular description region is limited to 255 characters. The Detail description field is an unlimited field so you can add as much detail as needed.
	Makes a copy of the current object which you can then edit as required.
	Adds an existing object to the current field

Status Icons	Graphically depict assessment results. For example:  Depending on the object that was assessed, can indicate Pass, I agree, Completed, or Meets Guidance  Depending on the object that was assessed, can indicate Pass with noted exceptions, I agree with noted exceptions, Requires Documentation, Requires Additional Analysis, Requires Evaluation  Depending on the object that was assessed, can indicate Failed, I do not agree, Out of Tolerance  Indicates that the assessor had no opinion  Indicates that there is no action needed  Indicates that an assessment has not been started

Component Statuses

The following list shows statuses that are possible, but depending on your business processes, and the component type, you might not see all statuses. For example, Review or Approval might not be required in your workflow.

Status	Description
New	The component has been created and saved.
In Review	The component has been submitted and is awaiting review by the reviewer delegate.
Awaiting Approval	The component has been reviewed and is awaiting approval by the approver delegate.
Active	The component has been approved and is in use

Work in Progress	The component has been modified and saved, and the owner is still working on it. After an owner submits a component, the component enters the review or approval workflow process and transitions to In Review or Awaiting Approval. The component becomes Active after it has been reviewed and approved. A component is also in Work in Progress status when it has been rejected at either the review or approval stage.
Retired	The component is no longer in use but still exists in the database and can be reactivated if required.
Reported	The component has been identified and submitted and is awaiting validation to disposition the item. This is used for proposed risks and issues.
Open	Used for issues. It is a current issue that is being worked.
In Remediation	Used for issues. A remediation of the issue is in progress.
Closed	Used for Issues. The issue is no longer current. No additional work will be performed against the issue.
On Hold	Used for issues. The disposition of the issue is on hold and is currently not being worked.

Common Tasks

The following are tasks that are common to most components:

- Working with Delegates
- Working with Attachments
- Working with Versions and Revisions
- Managing Objects
- Creating Issues for Objects
- Creating Object Classes

Delegation Explained

Delegation allows you to set up and assign responsibilities including approving, owning, or reviewing components in a work flow. You can delegate to a specific user (for example, jdough), or to a role (for example Internal Auditor.) You can track any delegate changes you have made such as changing or deleting a delegate from a component. When you modify the delegates for a component, a new revision of the component is created. Delegation provides:

- A robust and flexible security model with fine grain access control to fields and actions based on state. For information on state based security, refer to the Governance, Risk and Compliance - Fusion Editions Implementation Guide.
- Multiple individual and group roles for a responsibility (for example, Owner and Reviewer)
- Extensible responsibilities to meet specific access requirements

Delegation drives the review and approval processes, and reduces the cost of review and approval. Exactly how the delegation flow works is determined by the Delegation model in use. The delegation model describes which roles are required to perform which tasks for which objects, and how they must perform them.

Specifying Delegates: Critical Choices

When specifying a delegate, you need to decide to whom you want to assign a given task. To begin, select the + icon in the Delegate region for the component, then select a type:

Choose	If
User	You want to select one or more specific users to perform a task.
Role	You want all users who have a specific role to be assigned this task. The number of users that must actually complete the task depends on how your GRC Administrator has set up your delegation model.

How can I tell if a delegate is required for an object?

If the Delegation region appears within the component page, you must specify at least an Owner. All other delegates are optional.

What happens if I do not specify a delegate?

If no delegate is assigned to a task (such as Approve or Review), then the task is

skipped and the object is placed directly into its final status, such as Active.

How do I know if I am the delegate for a task?

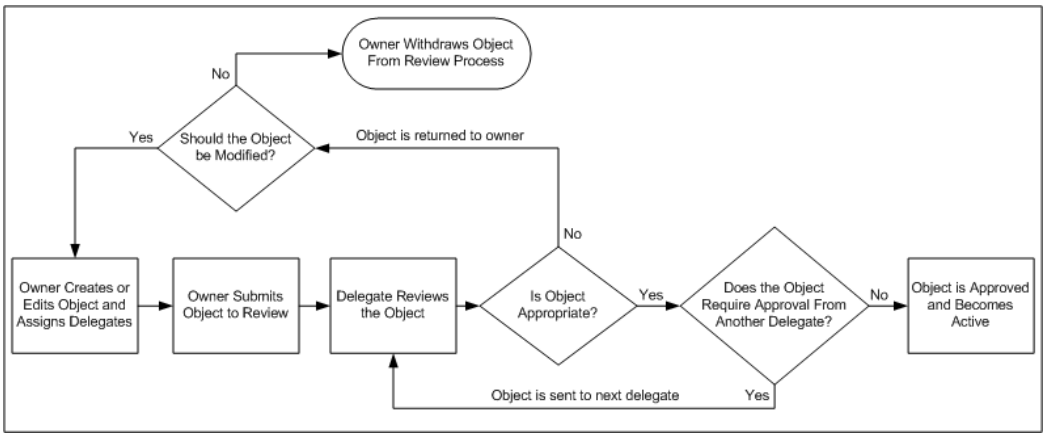
If a task is delegated to you, it will appear in your worklist and a description of the required task will appear in the Type column. For example, if the object has a task of Review Required, you would select the object, click the Edit button, and review the object.

What happens after a delegate approves or rejects an object?

If the object is approved, it is either passed to the next delegate (if additional reviews are required) or it is placed in it final state such as Active or Retired. If the object is rejected, it is sent back to the owner, who can either modify the object and resubmit it, or they can withdraw the component, which terminates the review process.

Objects stay in Active or the current status until they are modified, in which case, the object owner and the owners of all related components are notified of the change and the review and approval process is repeated. Once an object is no longer required it is retired.

A typical delegation work flow for an object would be:



Attachments Explained

Attachments are documents that can be used to associate supporting documentation with components. Attachments can be any document format including URL references, documents produced from many popular software applications, or other formats available to an organization. Attachment examples include:

- Business process narratives
- Business process flow charts
- Control test instructions

- Supporting issue remediation documentation

Versioning and Revisions Explained

Versioning Explained

When managing any component, you can view a complete version and change history of the component back to its creation. The change history displays previous versions, previous revisions, who made the changes, when the changes were made, and the status.

On initial creation, a component's default version date and first revision date are set to the current date. You can override the version date and set it to a date in the future. The future dated version becomes the active version on the appropriate date. You can also create a new version of a component after its initial creation at any time. The new version is a copy of the existing version details. The new version can also be a future dated version or you can except the default of the current date.

Revisions Explained

A new revision is created every time a component in Active status is created or changed. This provides an automatic audit log to the changes related to the component and, if specified in the delegation rules, invokes notifications and approvals. The revision date is automatically set to the system date and cannot be changed. You can compare across multiple revisions, print, and export the compare results.

What is the difference between a version and a revision?

Revisions are created automatically by the application whenever you modify an object. For example, if you change the Reviewer delegate on a risk, when you save the risk, a new revision is created.

You create new versions manually, they are not created automatically. For example, if you know that a government regulation is going to change on a certain date, you can create a new version of the current process that includes the new regulation, and specify that the new version will take effect on the same day as the regulation.

Managing Objects Explained

Most objects have a page from which you can manage them. Managing objects consists of many tasks, and the tasks that are available to you depend on your role. For example, if you have the GRC User role, you might be able to view the information on Summary and Definition tabs, but you will not be able to edit the object.

Creating Issues: Critical Choices

Issues are defects or deficiencies that are detected for an object. Although you can create

issues from within Issue Management, doing so is limited to only those roles that have access to Issue Management. You will usually create issues directly in the object. When creating an issue for an object, consider:

- To which class does this issue belong? There is a seeded issue called Financial Governance, but the options available in this field change based on your business processes and how your GRC Administrator has defined the classes.

- How serious is the issue? Is it a significant defect, a minor gap in functionality, or is it an issue that can be fixed with improved documentation?

Creating Classes: Critical Choices

An object class provides categorization for that type of business object and also provides defaults. For example, when you create a risk class, you must specify an analysis model. Then, if you want different analysis models to be used by different classes of financial compliance risks, you can identify a new class and analysis model for that class. You can create as many classes of a object type that you need.

When creating a new class, consider:

- What is an appropriate code for this class? The code can be anything you want, but it must be unique.

- What name should be assigned to this class? You can assign any name to the class that you want, but it should be relevant to your business needs.

- Which business component is the class for? Your GRC Administrator defines the business components you can chose from. These must be defined before you can define a class.

3

Perspective Management

Perspective Management Explained

Managing a perspective can entail:

- Creating a new perspective or perspective items
- Editing the hierarchy definition
- Creating or editing new perspective items. For example, there is a default perspective called Organization that is seeded in the application, but is empty and must be populated.
- Duplicating an existing hierarchy
- Creating a new version of a hierarchy, page 2-20
- Notifying a delegate that an action is required, page 2-18
- Creating an issue for a hierarchy, page 2-20
- Creating assessments to certify perspective hierarchies
- Completing assessments to certify perspective items. For example, in the Financial Governance module, you might perform certification for the organization perspective, which includes reviewing the processes, risks and controls within the organization
- Retiring or reactivating a hierarchy
- Creating a perspective class, page 2-21

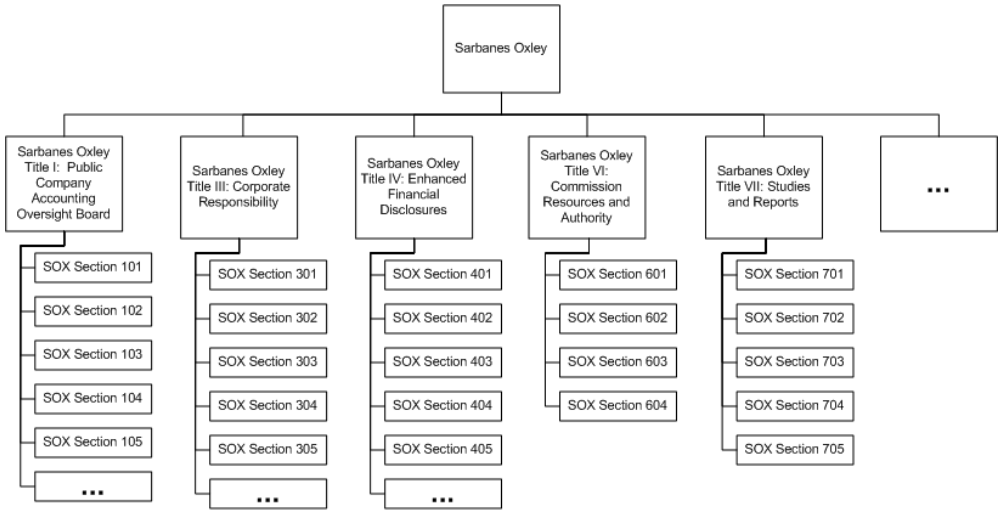
Creating a Perspective Hierarchy: Points to Consider

Before creating a new perspective hierarchy, consider the class of perspective that you need to create. In addition to any perspective classes created by your GRC Administrator, there are five pre-seeded Perspective classes:

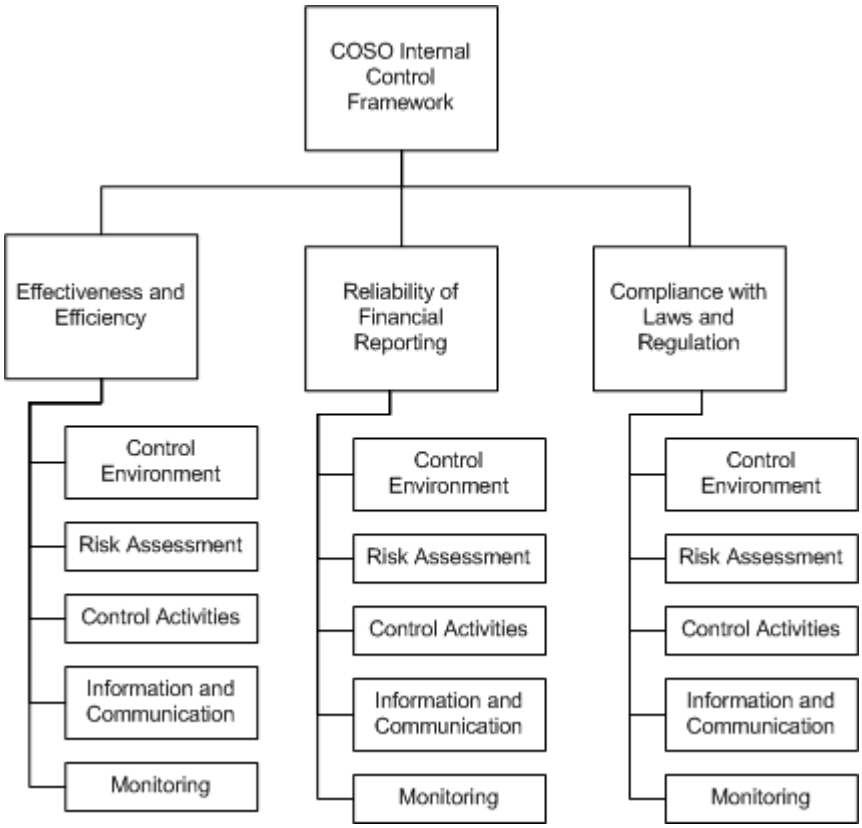
- Organization is used to describe a businesses internal structure. It is empty by default and you must populate it to describe your organization. For additional details on populating a hierarchy, refer to Creating Perspective Hierarchy Items Critical Choices, page 3-4.

  The Organization perspective is required for the Financial Governance Process and optional for other components. For the Financial Governance module, the organization perspective is not related to the other components. However, you can relate any perspective type to any component to achieve your desired points of view.

- Laws and Regulations is a class that describes Sarbanes Oxley regulations.



- Standard and Framework is a class that describes the COSO Internal Control Framework.



- Financial Governance Accounts is a delivered hierarchy, but it does not contain any perspective items. You can add accounts to fit your business needs.
- The Major Process class does not contain any hierarchy levels as that depends on how your company does business.

After you have selected a class, you populate the hierarchy by adding perspective items, page 3-4.

Do I need to specify delegates for each new perspective item created while constructing the perspective hierarchy?

Delegation is stored within the perspective item and therefore can be different across the perspective items within the hierarchy. Thus, you must specify delegates when adding a new perspective item to a hierarchy. Note, however that when associating an existing perspective item to a hierarchy, the delegates are already specified.

Can I create an issue for a hierarchy?

Issues are associated with perspective items, not the hierarchy. Although you cannot create issues for hierarchies, you can create issues for items, page 2-20 within a

hierarchy. If there is a problem with the hierarchy in general, create an issue at the highest level item in the hierarchy. Create an issue when you need to document any potential events that might affect the hierarchy. For example, you might create an issue on an Organization item if a department is missing or in the wrong place in the hierarchy.

How can I tell if a perspective has been modified?

Changes to perspective hierarchies and items are tracked using versioning and revisions. While managing a perspective, you can choose to view or compare revisions or versions in the Perspective Versions panel. Perspective items also have revisions which are tracked separately from the perspective hierarchy).

What is included when I duplicate an existing hierarchy?

Only the hierarchy structure is duplicated. Because the structure contains references to the perspective items, the items within the structure are not copied. The new hierarchy has delegation as defined within its delegation model. The roles or user assigned to responsibilities in the existing hierarchy are not copied into the new hierarchy. After the structure is duplicated, you can remove or add perspective items and delegates as needed.

Creating Perspective Hierarchy Items Critical Choices

When building the hierarchy, you indicate which items belong on the various levels of the hierarchy. The highest level within the hierarchy is called the root. Each item within the hierarchy is called a node. When creating a new node within the hierarchy, use one of the following methods:

- Create a new perspective item

- Create From Existing indicates that the entry in the hierarchy is a reference to a perspective item that already exists. When you choose Create From Existing, a link is created to the original item. If the original item is modified, the copy is also updated. You can only choose to copy from perspective items of the same class.

What is the difference between creating a child and creating a sibling?

When you create a child of the root, you create a subordinate level in the hierarchy. When you create a sibling of the root, you create another node at the same level in the hierarchy. Functionally, there is no difference between creating a child of a root and creating a sibling of an existing child; you choose the appropriate action for where your cursor is within the hierarchy. For example:

- Organization

- Division 1
- Division 2

If your cursor is on Organization, and you want to create Division 2 at the level shown, you would select Create Child. If your cursor was on Division 1, then you would select Create Sibling.

Managing Perspective Items

You can manage perspective items outside of a hierarchy. This is useful when you have defined multiple hierarchies that share the same perspective item. For example, you might have two perspectives for Standards and Framework Hierarchy, one for COSO and one for COBIT. Say that both hierarchies contain a perspective item of Effectiveness and Efficiency. If you need to change something on this perspective item, you can manage it directly instead of via the hierarchy.

Managing a perspective item can consist of:

- Modifying the item definition, which can include modifying delegates
- Creating an issue, page 2-20 Issues are used to identify any kind of deficiency for the item. For example, the delegation may be incorrect for the item such as an incorrect owner or assessor is specified. The issue could also identify a problem with a user defined attribute field or an attachment.
- Creating a new version or revision, page 2-20
- Retiring or reactivating an item

Perspective Assessments Explained

How do I perform an assessment for a hierarchy?

Create a certification assessment for a hierarchy when you need to certify the hierarchy. Performing an assessment is a two-step process:

1. Initiate the assessment. You can initiate assessments either through the Assessment Tool or from the Manage Perspective Hierarchies page. In the Manage Perspective Hierarchies Search Results region, select your hierarchy, then click the Create Assessment button.
2. Complete the assessment. Once the assessment is initiated, the users who are assigned to the assessment receive worklist entries. If you are the assignee, there are different ways in which you can complete the assessment:

- Click the entry in your worklist to display the Certify Perspective page where the assessment results are recorded.
- While managing the perspective, select the Assessment tab, then click the Complete Assessment button
- Complete the perspective certification from the My Assessment page.

Related: Certification process, page 3-6

Assessment Management Explained, page 8-1

Perspective Certification Process Explained

In general, the certification process of a perspective is performed from the bottom of the perspective hierarchy to the top node. A parent node cannot be certified until all its subordinates have been certified. However, if you are delegated responsibility for the hierarchy and all of its subordinate items, you can certify the parent node and the result will also be recorded for all child items. The certification process is:

1. A user (usually the perspective hierarchy owner) creates an assessment to certify the perspective hierarchy.
2. Worklist entries are created for the delegates who are assigned the assessor responsibility for the perspective items within the hierarchy.
3. A worklist entry is sent to the delegates assigned to perform the certification activity for the lowest level within the hierarchy. The certification process controls when it is appropriate for the assessors at each level to complete the certification. The state of the certification results at this time is Not Started.

   Tip: On the Certify Perspective page, only certify actions for the items that you own and the subordinate items that have already been certified are displayed. All subordinate perspective items must have the certification completed before moving up to the next level within the perspective hierarchy.

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

4

Risk Management

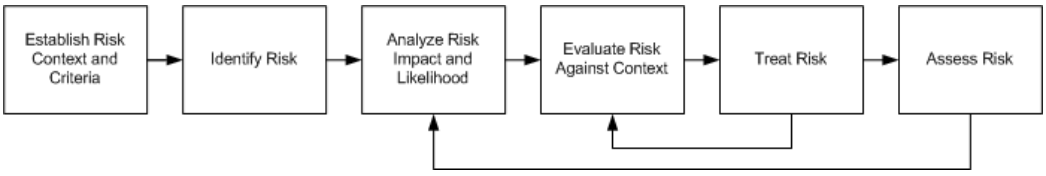
Risk Management Explained

Risk management includes the following tasks:

- Viewing metrics on the Risk Overview dashboard. Metrics can include risks by context, tolerance, significance and other reports that are available to your business.
- Proposing a risk
- Creating a risk
- Creating an event
- Creating a consequence
- Performing risk analysis
- Evaluating a risk
- Treating a risk
- Assessing a risk
- Performing risk administration tasks
- Creating issues for risks, page 2-20
- Managing risk versions and revisions, page 2-20
- Creating new risk classes, event classes, consequence classes and proposed risk classes, page 2-21

Risk Lifecycle Explained

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



- Risk Context: The risk context defines the general parameters for how risks must be managed and the scope for the enterprise risk management process. The Risk Context should include the organization's external and internal environment and the purpose of the risk management activities. For example, when an organization is defining their Risk Context, they should establish their overall strategies, objectives, goals, scope, and the understanding of the parameters for the risk activities.

- Risk Identification: Determining risk classification and associations

- Risk Analysis : Understanding the nature of and deducing the level of the risk

- Risk Evaluation: Comparing the level of the risk against risk criteria. The risk criteria are the terms of reference by which the significance of risk is assessed. Risk criteria can include associated cost and benefits, legal and statutory requirements, socioeconomic and environmental aspects, the concerns of stakeholders, priorities and other inputs to the assessment. The risk context is used when evaluating the risk.

- Risk Treatment: Selecting and implementing a method of addressing the risk with a goal of minimizing the risk's negative consequences

- Risk Assessment: Appraising the risk definition and evaluating the systems and business processes they support. Assessment types include certification and audit.

Proposing a Risk Explained

A proposed risk is a risk candidate; it may or may not become a formalized risk if the risk is not relevant or not significant to the risk context. A proposed risk may also be a duplicate of a known risk. A proposed risk has a likelihood and impact model associated with it. You can set the default likelihood and impact model for a proposed risk at the installation. Refer to the EGRCM Implementation Guide for details.

When proposing a risk, you must decide:

- What class will the new risk be?
- What is the likelihood that this risk will occur?
- What is the potential Impact or this risk?

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

What is the difference between creating and proposing a risk?

Any user role, including the GRC user, can propose a risk, but a proposed risk must be approved by a Risk Manager. Risks can only be created by users who have been given access to risk functionality as described in the Summary of Roles, page 2-1. The propose risk task is also available on the dashboard for users who do not have access to the risk work area. Once a risk is created, it follows the delegation process associated with the risk.

Do I always have to propose a risk before I can create one?

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

If a proposed risk is approved, is a risk automatically created from it?

No. If a risk manager approves a proposed risk, they must then manually create the new risk. In addition, not all proposed risks become actual risks. That is up to the discretion of the risk manager. Once a proposed risk has been submitted it is not deleted, even if the risk does not become a formal risk.

Creating a New Risk: Critical Choices

When creating a risk, consider:

- **The class that you need to use**

  The risk class points to the risk analysis model, which identifies the likelihood and impact models that are used to perform analyses on risks that belong to the selected class. There is one delivered risk class called Financial Governance Risk. This is a qualitative model which uses the Qualitative Likelihood Model and the Qualitative Impact Model. You may also have other classes available that use other models as defined for your business by your GRC Administrator.

- **The context for the risk**

Risk Management Context is used to:

- Set risk criteria and weighting against corporate performance objectives
- Set tolerance thresholds and significance scales

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

You may also have other contexts available that use other models as defined for your business by your GRC Administrator.

- **Any events or consequences that are associated with the risk**

  Determine if you need to associate any events or consequences to your risk.

- **Any perspectives associated with the risk:** Depending on how your GRC Administrator has configured risks for your business, there might be a perspective related to your risk.

- **Additional details required by your business process**

  If your GRC Administrator has added user defined attributes (UDAs) to your risk definition, they will appear in this section. Refer to the EGRCM Implementation Guide for details regarding UDAs.

Editing Related Controls Critical Choices

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

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

secondary control or to another key control.

- Monitoring: A control that monitors one or more related controls. It is used for management assessment, for example, assessing a monitoring control and not assessing its related key control or related secondary control. A monitoring control cannot be related to a subordinate control or to another monitoring control, and does not have a subclass.

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

- Redundant: Controls that institute the same controls as the key control.

- Mitigating: Controls that are currently eliminating risk for a process.

See also: Delegates, page 2-18

Creating a New Event: Critical Choices

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

- What is the event class? The delivered choice for the Financial Governance module is Financial Governance Event, but your GRC Administrator can create other classes of events.

- What likelihood model is most appropriate for this event? The default likelihood model is qualitative, but your GRC Administrator can define other models.

- What is the likelihood that this event will occur? The values that you can select from are determined by the likelihood model that you chose.

- What are consequences of this event occurring? Select an existing consequence that describes the possible outcome or impact of the event. You can associate more than one consequence. The possibilities can be positive or negative, and can be expressed qualitatively or quantitatively.

See also: Delegates, page 2-18

Creating New Consequences: Critical Choices

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

- What impact model is appropriate for this consequence? The impact model contains the criteria for weighing the importance of the event consequence to the risk in the case the event occurred. The default impact model is qualitative, but your GRC Administrator can create other models.

- If this event occurs, what could the negative or positive outcome be to the business objectives? The options you can select change based on the impact model that you selected.

- How should the consequence be classified? The class is used to organize the consequences, for example, for searching or reporting. There is a delivered class of Financial Consequence, but your GRC Administrator can create additional classes.

See also: Related Controls, page 4-4

Risk Analysis Explained

Risk Analysis Explained

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

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

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

- Transform risk data into decision-making information

- Evaluate impact, probability, and time frame

- Classify and prioritize risks

Risk analysis provides the basis for risk evaluation and decisions about risk treatment. There are two types of risk analysis:

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

- Semi-Quantitative: Semi-quantitative analysis provides ability to associate numeric values to qualitative likelihood and impact scales.

Risk Analysis Process

The Risk Analysis Process is:

1. Define and manage the risk analysis models, which includes the analysis formulas to be used within a risk analysis activity. A risk analysis model is a many-to-one relationship with risk class. That is, one risk class is associated to one risk analysis model, but one risk analysis model can be associated to many risk classes.

2. Define risk formulas by utilizing formulas that are available in the system.

3. Begin the risk analysis activity to identify the risk level.

Create Analysis: Critical Choices

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

- **Which likelihood model is appropriate for this analysis?**

  Risk analysis models provide definitions of risk formulas and add dimension to the risk analysis. The likelihood model contains the description or numeric weight of the probability of frequency to be applied to a risk during analysis. The likelihood model is associated with the risk class that you choose. There is a seeded Qualitative likelihood model, and you can create your own additional models.

- **Which risk likelihood is most appropriate for this analysis?**

  The risk likelihood options that are available are determined by the likelihood model you have specified.

- **Which impact model is most appropriate?**

  The impact model contains the criteria for weighing the significance of the event's consequences if the event actually occurs. Select the model that you want to use. There is a seeded Qualitative Impact model, and you can also create your own impact models.

- **What is the potential impact of this risk?**

  Options change based on which Impact Model you have specified. You can only associate Impact Models which are the same type as the Impact model type.

- Which risk specific formula is appropriate for this analysis?

  The types of Risk Formulas available in the system are:

  - Product: Product is the only type that can be used for Qualitative Analysis. When you select Qualitative as the analysis type, the Risk Level Formula

defaults to Product. The Risk Level Formula for Product is Likelihood x Impact.

- Weighted: Weighted Product is only available for Quantitative Analysis. The formula used is:

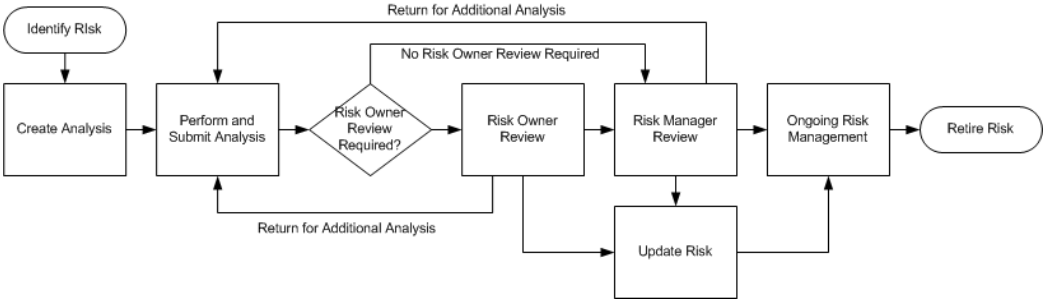
  Risk Level = ((Impact x weighting factor)x) x ((Likelihood)y)

  Where you specify the Weighting Factor, Power X and Power Y.

See also: Risk Administration, page 4-10

Analysis Process Flow

Depending on your business process, after an analysis is created, it might have to go through a series of reviews and additional analysis. A typical analysis process flow might be:



Risk Evaluation Explained

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

You can only perform risk evaluations after the risk context and risk criteria are associated to a risk and risk analysis has been performed. You can perform multiple risk evaluations. You typically perform risk evaluation after the risk criteria has been modified, risk analysis has been modified, or on a scheduled time increment. The appropriate user is notified when a risk has been modified and they can decide if it is appropriate to perform an evaluation.

Creating an Evaluation Critical Choices

When creating an evaluation, consider the following:

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

Risk Assessments Explained

Creating a Risk Assessment Critical Choices

When creating a risk assessment, consider the following:

- What type of assessment will be performed?
- To whom will the assessment be assigned? Select a delegate, page 2-18 that is associated with the risk.

Related:Assessment Management Explained, page 8-1

Risk Treatments Explained

Creating a New Treatment Plan Critical Choices

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

- How will the treatment plan be used?
  - In Use: Is the plan currently in use?
  - Target: The events that the treatment being applied should target in order lower the risk level to an acceptable level.
- What , if any, treatments should be performed? A treatment plan is used to identify, evaluate, and implement options for treating risks.
- What are the residual likelihood and impact of the treatment plan? When one or more Control Components are associated with a Risk, and the Control has the Risk Impact capability enabled, residual (controlled) risk values are calculated from the sum of the related control impact values.

See also: Delegates, Creating a New Treatment Critical Choices

Creating a New Treatment Critical Choices

After risk analysis and risk evaluation have been performed, create a risk treatment to

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

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

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

See also: Delegates, page 2-18, Related Controls, page 4-4

Risk Administration

Creating an Analysis Model Critical Choices

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

- What type of analysis will be performed? You can choose qualitative or semi-quantitative.
- What likelihood model should be used? The options you see here are based on the analysis type you chose.

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

    Risk Level = ((Impact x weighting factor)x) x ((Likelihood)y)

    You must enter the weighting factor, as well as the power for x and y.

Create Likelihood Model: Critical Choices

When creating a new likelihood model, consider the following:

- What type of model will it be? You can choose Qualitative or Semi-quantitative
- Which likelihood model will be used?
- Which impact model should be used?

Create Impact Model Critical Decisions

The impact model contains the criteria that is used to weigh the significance of the event consequence in relation to the risk, in the case the event occurred. When creating the impact model, you should consider:

- What type of model should be used? Options are Qualitative and Semi-Quantitative.
- What details should be specified for the impact? Options you will see include:

Field	Used with Models of type
Sequence	Qualitative, Semi-Quantitative
Low Value	Semi-Quantitative
High Value	Semi-Quantitative

Label	Qualitative, Semi-Quantitative
Output Rating	Semi-Quantitative

Creating a Risk Context Model Critical Decisions

The Risk Context Model defines how the Risk Rating value and Risk Significance value is derived during the risk evaluation activity. When creating a risk context model, consider:

- Which Risk Significance Model should be used? The Risk Significance Model determines the risk significance value using the overall risk rating from the risk evaluation activity. The Risk Significance Model uses a Risk Rating Minimum and Risk Rating Maximum range to determine the Risk Significance value.
- What is appropriate Risk Context criteria? Criteria is a user defined value that is used by the Risk Context Model. After you define the Risk Criteria value it can be selected by the Risk Context Model.
- What details are required for the model? You can include:
  - Value: Values can be either strings (such as High, Med, Low) or integers (1-9).
  - Tolerance: Risk-Tolerance is the acceptable level of risk when compared to the possible benefits. Options for risk tolerance are Acceptable, Monitor, or Treat.
  - Rating: The rating is the tolerance score and can be any number between 1-100.

Risk Significance Models Explained

The Risk Significance Model determines the Risk Significance value using the overall Risk Rating from the Risk Evaluation activity. The Risk Significance Model uses a Risk Rating Minimum and Risk Rating Maximum range to determine the Risk Significance value. For example: the Risk Rating will be an integer between 1-100, but you may only want five Risk Significance values. You would need to create five rows in the Risk Significance Model using the Minimum and Maximum values.

5

Control Management

Managing Controls Explained

Managing controls can consist of the following tasks:

- Viewing metrics on the Controls Overview dashboard. Control metrics can include control counts by class or trend, as well as other reports that are available to your business.

- Creating New Controls: Create a new control when you require a policy, procedure or other action to mitigate risks

- Creating Control Test Plans and Instructions: A control test is used to test the effectiveness of the control and to determine if additional treatment is required. The test plan and instructions document the steps to follow to perform the actual testing.

- Creating Control Assessments: A control assessment is the review of policies and procedures that is performed to ensure that the controls are still effective and appropriate.

- Creating Control Issues, page 2-20: Create an issue to document any potential defects or deficiencies with the control itself or with specific assessment activities.

Creating New Controls Critical Choices

When creating a control, consider the following:

- To which class does the control belong? Financial Governance Control is the delivered class, but you can create other classes, for example, QA Control class to document quality assurance controls.

- What type of control are you creating? There are three control types:

    - Preventive
    - Corrective
    - Detective
- What will the implementation method for the control be? You can select:
    - Manual: A manual control requires human intervention. For example, a manual control might be that an insurance policy must be reviewed for adequate coverage before annual renewal.
    - Automatic: The control is automatically evaluated in a tool external to EGRCM. Automated controls do not require human intervention; for example a control that specifies that an Accounts Payable system requires top executive approval of all payments over a certain dollar amount, or a control that prevents the same user from both creating and approving an expenditure.
- What is the potential cost of the control?
- What assertions will this control evaluate? Assertions are statements of presumed facts about the status of a business process. For example, assertions can be made that financial assets exist and that financial transactions have occurred and been recorded during a period of time. Assertion types include:
    - Existence/Occurrence
    - Completeness
    - Valuation/Allocation
    - Rights and Obligations
    - Presentation/Disclosure
    - Accuracy
    - Cutoff
- Will this control be in scope for audit testing or assessments? Does this control require a test plan?

Test Plans Explained

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

Creating Test Plans Critical Choices

When creating test plans, you need to determine:

- What type of assessment will be used? Choices are:
  - Operating Assessment: Used to determine if the control is operating effectively and operating as designed.
  - Certify: Used to determine if the information in the assessment is accurate and complete.
  - Design Assessment: Used to determine if the control is designed effectively.
  - Audit Test: Use to determine whether or not the control mitigates the risk and meets audit guidelines.
- What test instructions are required? Will the test instructions be manual or automated? Automated instructions describe steps that are performed in an external automated tool.

Creating Manual Test Instructions Explained

When creating manual test instructions, you need to determine what test instructions should be included. For example, if you have a control that requires that a board of directors meeting includes a monthly briefing for non-routine events and transactions, manual test steps might include:

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

Creating Automatic Test Instructions Explained

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

Editing Definitions Explained

When editing a definition, you can:

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

- Add or remove delegates
- Add or remove perspective items to the control.
- Add existing or create new related components to the control: You can add or create related components appropriate for the class of the control. You can either associate an existing component, or create a new related component

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

See also Creating a Control, page 5-1 and Creating a Component, page 6-1

Control Assessments Explained

A control assessment is the systematic review of processes to ensure that controls are operating and designed effectively and appropriately. An assessment can be part of an assessment batch defined within the assessment tool, or it can be a single assessment performed just for one specific control.

A control assessment includes executing the appropriate test plans for the type of assessment being performed. In performing the testing, the results are recorded for each step and instruction within the test plans as well as providing evidence of that testing.

Creating a Control Assessment Critical Choices

In addition to using the Assessment Manager tool, you can also create an ad-hoc assessment from within Control Management, on the Assessment tab. When creating an assessment, you must decide what kind of assessment activity is required. You can use different control types, so the activities required vary based on how the class was configured. Note that you can choose not to require certain assessment activities, but you cannot create new assessment activity types. Refer to Initiating Ad-hoc Assessments, page 8-3 for a list of assessment activities that you can perform individually or in various combinations within an assessment to assess controls

When completing the assessment, you need to decide:

- Has this control successfully passed the assessment?
- If the control has not passed the assessment, do you need to create an issue to address the situation? See also Creating Issues

Refer to What do the assessment result options mean?, page 8-4 for details.

6

GRC Component Management

Managing Components Explained

Managing GRC Components can include the following tasks:

- Creating new GRC components
- Viewing a matrix of components and the objects to which they are related.
- Creating action items
- Managing versions and revisions, page 2-20
- Creating issues, page 2-20
- Managing assessments
- Viewing metrics on the GRC Overview dashboard, including action item activity, overdue activities, and another reports that are available to your business.
- Managing GRC component classes, page 2-21

Creating GRC Components: Critical Choices

When creating a new GRC component, consider the following:

- To which class will the new component belong? For example, the delivered class of Financial Governance Process is appropriate for the Financial Governance module, and you can create other classes as needed. Refer to Managing Classes, page 2-21 for additional information.
- Is this component in scope for audit testing and assessments? These indicators are used during assessment as selection criteria. When this criteria is used during

assessment, only those components that have been selected for the activity are brought into the assessment.

- If there is a perspective associated with this component, is it correct and complete? The Perspective region displays all perspectives that are configured for the type of component being created. You can view and manage the perspective items that are associated with the component.

- Should any other components be associated to the component that you are creating? For example, you might want to associate a risk or another type of GRC Component.

- Are there any delegates who will be responsible for reviewing or approving this component? Refer to the description of the delegation process, page 2-18 for details.

What is the matrix used for?

The Matrix displays associated components, risks and controls in a tabular view so that you can immediately visualize the relationship between risks and controls for the component. The matrix also provides navigation into related components.

When would I create an issue for a component?

Create an issue for a component when there might be a problem. For example, if you created a Year End Closing Process, a possible issue might be that there are unsigned legal documents that are required for year end financial statements to be approved

Assessments Explained

Performing Assessments: Critical Choices

When creating a new assessment, consider the following:

- What type of assessment will be performed? The type of assessment you can perform varies depending on the control type. Refer to Initiating Ad-hoc Assessments, page 8-3 for a complete list of assessment activities that you can perform individually or in various combinations.

- Who will be responsible for performing the assessment?

How do I complete an assessment?

If you are the delegate to whom an assessment is assigned, there are two ways you can complete the assessment:

- Access your My Assessments page from the Tasks region of your home dashboard.
- While managing the component, select the assessments tab

Refer to What do the assessment result options mean?, page 8-4 for details.

Action Items

Creating Action Items: Critical Choices

Create an action item for a component when additional tasks are required. For example, if you have a Process component for the Year End Closing Process, you might require a task to verify that certain tax documents are included in the year end reporting.

When creating a new action item, consider the following:

- What is the assignee expected to do? Describe in details how the action item must be accomplished. For example, say that you suspect that there some details of a recent acquisition were not recorded. The instructions might be: "Contact the finance department and obtain the details of last quarter's XY merger, and verify that they are recorded in the closing statements."
- What is the time frame in which this action item should be accomplished? Specify:
  - Due Date: When creating an action item, specify the date on which work on the action item must be completed.
  - Target Completion Date: When editing an action item, the target completion date is entered by the assignee when they are projecting a new date for the action item. This field is only available when editing, not creating, action items.
- What is the priority of this action item? The priority is reported in the metrics reports.
- What is the current progress of the action item? You can choose:
  - Assigned: The action item has been assigned, but work has not yet begun.
  - On Target: The assignee is working on the action item.
  - Delayed: Work on the action item will not be completed by the due date.
  - Blocked: No work can be done on the action item.
  - Completed: Work on the action item is finished, and it has been marked as complete.

- To whom should this action item be assigned? This is the delegate who is responsible for completing the action item.

What is the difference between a Target Completion Date and a Due Date?

The Due Date is set when the task is created by the owner of the action item , and is the date by which the activity should be completed. Target Completion Date is entered by the user assigned to do the work as when they expect to complete the work. This is used to report the progress of the activity. For example, if problems occur, an assignee can report their progress as Blocked and update the target completion date. Assignees cannot change the due date.

7

Issue Management

Issue Management Explained

Issue Management can include the following tasks:

- Viewing metrics on the Issues Overview dashboard, including open issues by severity, issues awaiting remediation, and other report that are available to your business.
- Creating issues
- Creating remediation plans

There are two ways to manage issues:

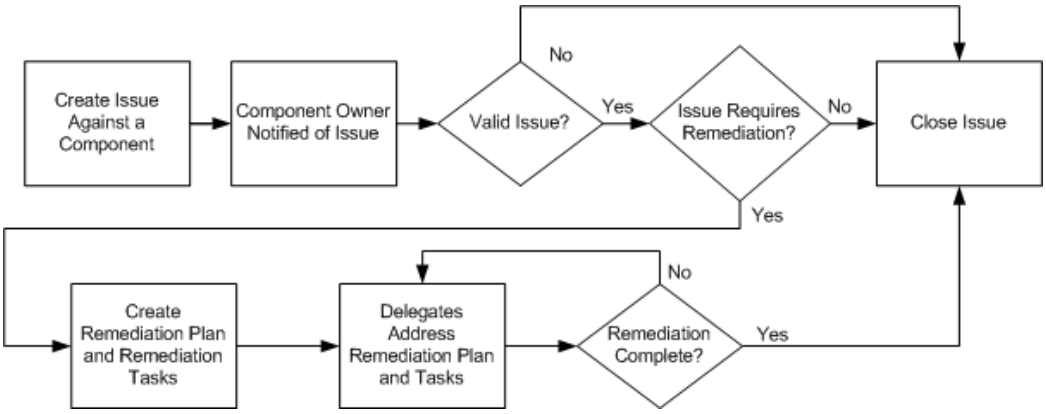
- Via issue management as described in this section
- In the context of the component definition, action, or assessment, page 2-20

Issues Explained

Issues are defects or deficiencies that are detected for an object. Issues can arise from within the context of the GRC business process. Issues are associated with and reviewed in the context of their related component. Delegates and other relevant attributes are inherited from the related component.

Issue Lifecycle Explained

The lifecycle of an issue is as follows:



1. The issue is created and the issue owner is set to the owner of the component that the issue is raised against.
2. A worklist item is created and assigned to the component owner.
3. The issue owner (which may or may not be the component owner) validates the issue and determine the disposition of the issue. They can determine that the issue is valid, close the issue, or put it on hold.
4. If the issue is valid, the owner decides if a remediation plan is required to address the issue.
5. The remediation plan is defined and tasks are identified and assigned to the appropriate delegates.
6. A worklist entry is created for the delegates assigned to complete remediation tasks
7. Delegates complete the remediation tasks.
8. When all tasks are completed the remediation plan is marked complete.
9. After the remediation plan is completed, this Issue is closed.

Creating Issues Critical Choices

Create a new issue to document reported defects or deficiencies against any component or its related activities, including risks, controls, GRC components, or perspectives. When creating an issue, consider the following:

- To which class will the issue belong? The class is used to categorize the issue. There is a seeded class of Financial Governance Issue, but users with the appropriate roles can create other classes specific to your business, for example, you might have a Company Policy Issue.

- How severe is the issue? The severity that you choose is used to help classify the issue, and can be used as a search or sorting aid.

- Are there any specific components related to this issue? When you create an issue from the Issue Management page, you must specify the component to which the issue is related.

Editing an Issue Critical Choices

When editing an issue, consider the following:

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

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

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

- Does this issue require remediation? If so, create a remediation plan to address the issues. Remediation plans are used to document responses to an issue and to track the work required to resolve the issue.

- What is the financial impact of this issue? The financial impact of the issue is used to quantify, in monetary terms, what the issue cost is to the organization. It is not used in any calculation or roll-up. This is measured in the currency specified for the related component.

- What is the chance that this issue will recur? Can this issue be closed? Close an issue when:

  - All remediation plans tasks have been completed

  - The remediation plan has been set to completed

Creating Remediation Plans Critical Choices

When creating a remediation plan, consider the following:

- What class is the remediation plan? There is a seeded Financial Governance Remediation Plan, but users with the appropriate roles can create additional classes. The class is used to categorize the new remediation plan.

- What is the cost of the remediation? Specify how much it would cost to implement the remediation plan.

- How much progress has been made on the remediation plan? Are the remediation tasks on schedule (On Target), not on schedule (Delayed), or are you unable to make progress due to external forces (Blocked)? Progress for the remediation plan is derived from the status of the tasks. Progress for the issue remediation is derived from the status of the tasks for all remediation plans for the issue.

- What is the priority for completing this plan?

- Have any of the associated remediaion tasks been completed and can they be marked as such?

What is the difference between a Target Completion Date and a Due Date?

The Due Date is set when the task is created by the owner of the remediation plan, and is the date by which the activity should be completed. Target Completion Date is entered by the user assigned to do the work as when they expect to complete the work. This is used to report the progress of the activity. For example, if problems occur, an assignee can report their progress as Blocked and update the target completion date. Assignees cannot change the due date.

Creating a Remediation Task Critical Choices

When creating a new remediation task, consider the following:

- What is the priority for completing this task? The priority is taken into account for issue reporting.

- How much progress has been made on the remediation plan? When editing a task, the delegate to whom the task is assigned updates the task with the current progress, specifying if the plan on schedule (On Target), not on schedule (Delayed), or unable to be worked on due to external forces (Blocked).

- What is the current status of the task? When editing a task, the delegate to whom the task is assigned decides if the task is in progress (Active) or if it can be marked Complete.

- To whom should this task be assigned? Tasks are assigned to a delegate, that can be any user or role that is specified as a delegate for the remediation plan. The assignee is the only delegate that is responsible for tasks.

- What specific task needs to be performed? For example, say that you created an issue during an operational assessment of a control because there are no instructions for the test plan, which caused the assessment to fail. The remediation

plan is to correct the control test plan definition, and the remediation tasks might be:

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

8

GRC Tools

GRC Tools Explained

GRC Tools consist of:

- Assessments, page 8-1
- Surveys, page 1-5

Assessment Management Explained

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

- Creating assessment templates
- Creating assessment plans
- Assigning delegates to assessment templates and plans, page 2-18
- Initiating and completing assessments
- Reviewing assessment results
- Closing assessments

Creating Assessment Templates: Critical Choices

An assessment template is a collection of assessment activities. Assessment templates also display user-defined component relationships and their related assessment

activities. When creating an assessment template, consider:

- For which application module will the template be used?
- What is the primary component that will be assessed?
- What type of assessment will be performed? For example, you might need to prepare Financial Year End or Financial SOD assessments
- What activities will be performed during this assessment? Depending on the component you have added, you can choose activities such as Audit Test, Operating Assessment, Design Assessment or Certify.

Assessment Plans Explained

Creating Assessment Plans Critical Choices

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

- With which component will this plan be associated?
- Which assessment template will this plan use? The options that you have to choose from are dependent on the component that you choose, and you can only select active templates.
- Does this plan require a survey template to be attached? A survey template can be included on any assessment activity for components.
- What selection criteria do you want to specify? This is what determines what will be assessed for the component that you chose. If you do not select any criteria, everything associated with your component will be assessed; selecting criteria limits what will be assessed.
- What perspective selection criteria do you want to specify? Entering a perspective in the selection criteria provides an additional filter of the data. For example, if you chose the organization perspective and select one of the child items within it, the assessment will only include the assessment components that are within the hierarchy of that perspective node.

What is the difference between an assessment template and an assessment plan?

An assessment plan is used to specify which components will be used in an assessment. The assessment plan references the assessment template, which is a collection of assessment activities to be used, including additional assessment criteria. Templates can

be applied to multiple assessment plans. When you initiate an assessment, you indicate which plan to use. You can use assessment plans repeatedly to initiate and complete new assessments.

Initiating Assessments Explained

When you initiate an assessment, you select an active assessment plan and choose the assessment activities that will be performed. If a survey template is associated with assessment activity, a survey is initiated. You can schedule an assessment's a due date and modify the delegates that have been assigned to the assessment activities during the creation of the assessment plan. You can also review and override individual objects from the assessment plan selection criteria.

Initiating an Assessment Critical Choices

When initiating an assessment, consider the following:

- Which assessment plan will be used for this assessment? The assessment plan contains the criteria for the assessment activities that are associated with the assessment template.
- What activities need to be performed? For example will this be an audit test or an operating assessment?
- What selection criteria is needed for this assessment? The assessment administrator who initiates the assessment can refine the plan selection criteria.
- What components will be assessed? The components that you can choose from are based on the information model's primary component and are filtered depending on the application module.
- What delegates are required? If the activity is of type Survey, the owner is the component owner, not the assessor.

Initiating Ad-hoc Assessments

As part of managing objects such as risks, controls and GRC components, you can create ad-hoc assessments. Depending on the object you are creating, you can perform some or all of the following assessment activities:

- Operational Assessment: Enables the reviewer to determine if the object is operating effectively and as designed. Answers the question: "Is the object operating effectively and as designed?"
- Certification: Certification is part of the assessment process. All resources that have an active role in the accuracy of the assessment are typically required to provide an

answer to the certification statement and provide supportive comments to their answer. Answers the question: "Is the information in this assessment accurate and complete to the best of my knowledge?"

- Design Review: Enables the reviewer to determine if the object is designed effectively and meets the objectives. Answers the question: "Is the object designed effectively and does it meet the objectives?"
- Audit Test: Enables the reviewer to test if the object meets audit guidelines. Resources follow the audit guidelines that have been defined by the corporation. Answers the question: "Does this object meet audit guidelines?"
- Documentation Update: Enables the reviewer to determine if the object has the appropriate documentation required.

Completing Assessments Explained

Completing Assessments Explained

You can complete an assessment by selecting Complete Assessment from the Task list on the GRC Tools page. This invokes the My Assessments page, from which you can:

- Create an issue for the assessment
- View the hierarchy associated with the assessment
- Drill on the component to view details
- Click the Complete button to complete the assessment

You can also complete an assessment via the Manage Assessments page, from the Assessments tab of an object, or from the worklist on your home page.

Assessments are displayed as long as the assessment plan is active, even if you have completed it. The owner is the only person who can close an assessment.

What do the assessment result options mean?

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 the risks with noted exception.
- No Opinion: The reviewer has reviewed the object but does not have a definite answer of Pass or Fail.

- Failed: The object does not operate properly to mitigate the risk. The Assessment fails and you are presented with the option to create an issue within the workflow.

For Certify assessments

- I agree with this statement: The delegate completing the certification agrees that the information in the assessment is accurate.
- I agree with this statement with the noted exception: The delegate completing the certification agrees that the information in the assessment is accurate with noted exceptions.
- I do not agree with this statement: The delegate completing the certification does not agree that the information in the assessment is accurate.
- No Opinion: The delegate completing the certification either cannot or chooses 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.

Can I close an assessment?

Only the assessment owner can close an assessment. In most cases, this is either when the due date is reached or when all of the individual assessments within the initiated assessment batch are completed.

Managing Surveys Explained

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

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

- Managing survey versions and revisions, page 2-20
- Deleting surveys

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

Managing Survey Questions

Creating Questions Critical Choices

When creating survey questions, consider:

- What type of question will this be? You can choose 302 Organization Certification, or General, or any other question type that your GRC Administrator has created.
- What will the format of the question be? The format type for the question identifies how the responses to the question are presented. Options are:
  - Single Response: Radio buttons that present multiple options, only one of which can be chosen.
  - Single Response with Other, Please Specify: Radio buttons that present multiple options, only one of which can be chosen. One of the options is Other, Please Specify, which includes a text field where the respondent can enter an alternate choice.
  - Single Response Drop Down List: A list of values that presents multiple options, only one of which can be chosen.
  - Multiple Choice: Check boxes that present multiple options, from which respondents can select multiple options.
  - Multiple Choice with Other, Please Specify: Check boxes that present multiple options, from which respondents can select multiple options. One of the options is Other, Please Specify which includes a text field where the respondent can enter an alternate choice.
  - Multiple Choice List Box: A scrolling list box that allows users to select multiple values
  - Rating on a Scale: Radio buttons that represent a range of values. For example, if the question is, "How often do you use this tool?" The values might range from Always to Never.

- Numeric Allocation: Presents multiple options to which the respondent enters a number enters a number to quantify each option for the question. For example, if the question is, "What percentage of your monthly minutes do you allot for the following features on your cell phone? Answers must equal 100%" The values might be E-mail, Texting, Voice, and GPS, and the user is expected to enter a number for each option

- Open text: A text box into which respondents enter free-form text.

- What choice set contains the appropriate answers to the question? You can specify an existing choice set or create a new one. If you choose an existing choice set, you can edit it to suit your needs. For example, you can select a choice set that contains the values Yes and No, and create your own value of Maybe, or you could select the choice set of High, Medium, Low and delete Medium. You can then save any new combination of answers as another choice set for use in the future.

Managing Survey Choice Sets

Choice sets are a collection of answers to be used as a short cut for completing questions. For Example, a choice set could contain the answers: I agree, I Disagree or High, Medium, Low or Yes, No. The answers could be appropriate for a very large number of questions. Using choice sets provides reusability of answers as well as consistent recognition to the same answer across questions. Managing choices sets can consists of the following tasks:

- Creating new choice sets: To create a new choice set, either add existing answers to a new choice set, or click the Create New Choice button to create a new answer, then add that new answer to your new choice set

- Editing existing choice sets

- Duplicating choice sets: If there is a choice set that has similar choices to what you require, you can duplicate it then edit it to add new answers or delete answers that you do not need.

Managing Survey Templates

Creating a Survey Template Critical Choices

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

- What type of survey will this template be used for? Options include Financial Compliance, 302 Certification, General, or any other types that your GRC Admin has created.

- Do respondents require any special instructions for filling out the survey?
- Will the template have to be translated, and, if so, into what languages? Options include the languages that your installation is using. Note that this field is informational only, translation not automated, it is a manual task performed by the translators.
- What questions are part of the survey? You can create new questions or reuse existing questions.
- How do you want the survey displayed? You can format the survey by inserting page breaks at any point.
- Which delegates are required? For surveys templates, you can specify a Translator delegate, who will be notified that the template needs to be translated.
- Is the survey template what you are expecting? Use the Preview button to verify that the format and layout of the questions are as you intended.

What happens when I delete a survey template?

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

Survey templates can be retired while they are Active, however you cannot retire a survey template if there are surveys that use the template that are open to collect responses. Once a survey template is retired the assessment owner (and any other upstream delegates who have some type of an association to the survey) receive a notification that is displayed in the pending activities section of the dashboard or overview pages. For example, if a survey owner retires a survey, any business owners who are using the survey for an assessment are notified.

Translations Explained

You can specify that a survey template, including the questions associated to the survey, should be translated. Once a survey is translated, the system displays the survey based on the respondent's language preference. If the survey is not translated into the respondent's preferred language, it is presented in the base language for the installation.

Creating and Editing Surveys Explained

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

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

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

Completing Surveys Explained

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

Glossary

Action Item

Detailed tasks associated with a GRC component that identify some type of activity to be performed.

Application Business Component

The basic building blocks of an application module. The components represent the deconstruction of standard frameworks including COSO, COBIT, ITIL, ISO, AUSNZ and the link. Examples include; Risk, Control, Event, Issue, Process, Policy, and so forth.

Application Module

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

Assessment Activities

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

Assessment Survey

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

Assessment Template

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

Assessment Plan

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

Assessment Results

The summary of an initiated assessment and each individual object within the

assessment. You can view the status and delegation assignees of the assessment summary and each individual object within the assessment. You can view the assessment results of in-progress and completed assessments (assessments history).

Attachment

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

Choice Set

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

COBIT

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

Compliance Assessment

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

Consequence

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

Control

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

Control Assessment

The systematic review of processes to ensure that controls are operating and designed effectively and appropriate.

Control Stratification

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

Control Stratification – Key

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

Control Stratification – Monitoring

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

Control Stratification – Secondary

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

Control Stratification – Subordinate

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

Control Stratification – Compensating

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

Control Stratification – Mitigating

Controls that are currently eliminating risk.

Control Stratification – Redundant

Controls that institute the same controls as the key control.

Corporate Communication

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

COSO

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

Delegation

The act of assigning responsibility, authority, or power to someone.

Delegation Responsibility

Identifies the role to which the user is assigned for a particular GRC business component. Responsibilities identify a user's access to the data and the activities they can perform.

Distribution List

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

Duty Role

Duty Roles are the lowest level within the security hierarchical structure of roles. They represent the specific tasks performed with the EGRCM application and are the roles associated with specific functionality within the application.

Event

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

Framework Application Module

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

Frequency

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

General Survey

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

GRC Business Initiative

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

GRC Component

General purpose objects that can be defined as needed.

GRC Intelligence

Dashboards and business insight including executive level dashboards consolidating information across initiatives as well as business initiative specific insight.

Guidance

A set of guidelines or help principles which assist organizations in conforming to the regulation and enforcing the policy. Direction or advice to a decision or course of action. Guidance provides a set of guidelines which assist organizations in conforming to a regulation and enforcing the policy. Guidance can originate from external organizations separate from the policy marker or directly with the organization.

Impact

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

Impact Model

The criteria of weighing the significance of the events and consequences to the risk in the case the event occurred.

Impact Model – Qualitative

The risk analysis method utilizing the use of description rather than numerical methods to define the impact level of risk (for example, High, Medium, Low.)

Impact Model – Quantitative

Risk analysis method which utilizes the use of numerical methods to define the impact level of risk (for example, a dollar amount.)

Information Model

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

Inherent Risk

The pure risk that is intrinsic to the specific business objective without considering the impact of any related internal controls, established policies and procedures, or risk management practices.

Initiate Assessment

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

Issue

Reported defects or deficiencies against any business component such as risk, control, GRC Component, or perspective items.

Job Role

A collection of duty roles or other job roles that represent all the duties or tasks that a person in that specific job would perform. A user can be assigned one or more job roles to define their functional access within EGRCM.

Legislation (Law)

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

Likelihood

The probability or frequency of occurrence.

Likelihood Model

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

Likelihood Model – Qualitative

Risk analysis method which uses qualitative measures rather than numerical methods to define the likelihood level of risk

Likelihood Model – Quantitative

Risk analysis method which uses numerical methods to define the likelihood level of risk

Mandate

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

Monitor

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

Object Type

Identifies the individual components within the application. For example: Organization or Person.

Perspective

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

Perspective – Organization

The organization perspective defines your company's organizational structure.

Perspective Hierarchy

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

Perspective Item

The individual nodes that comprise the levels of a perspective hierarchy.

Policy

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

Procedure

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

Proposed Risk

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

Question Type

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

Regulations

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

Regulatory Audit

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

Remediation Plan

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

Remediation Task

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

Revision Date

The date on which an object was last modified.

Risk

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

Risk Analysis

The systematic process to understand the nature of, and to reduce the level of risk. Risk analysis provides the basis for risk evaluation and decisions about risk treatment.

Risk Context

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

Risk Analysis – Qualitative

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

Risk Analysis – Quantitative

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

Risk Analysis Model

The technique designed to quantify the impact of risk uncertainty.

Risk Assessment

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

made.

Risk Criteria

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

Risk Evaluation

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

Risk Identification

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

Risk Impact – Inherent

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

Risk Impact – Residual

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

Risk Impact – Target

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

Risk Level

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

Risk Treatment

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

Risk Class

The business objectives classification of a risk.

Security Roles

Refers to role given to a user to grant access.

Stakeholder

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

Stakeholder – External

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

Stakeholder – Internal

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

Survey

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

Test Instruction: Automatic

Test steps that are performed in an external automated tool.

Test Instruction: Manual

Test steps that are performed with human intervention.

Test Plan

Documents the steps required to perform a control test.

Treatment

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

Treatment Plan

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

Treatment Stratification – Compensating

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

Treatment Type – Risk Avoidance

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

Treatment Type – Risk Reduction

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

Treatment Type – Risk Sharing

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

User Defined Attribute (UDA)

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

User Defined Type (UDT)

Extends the definition of the base core object type. Each UDT may have additional attributes (UDAs) that are unique to it as well as different references to the other business components within the application.

Version Date

The date in which the object becomes active within the application.

Voluntary

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

Index

A

B

C

D

E

F

G

H

I

J

K

S

T

U

V

W