



THE
POWER
TO KNOW.

SAS[®] Enterprise GRC 6.1

User's Guide

The correct bibliographic citation for this manual is as follows: SAS Institute Inc. 2014. *SAS® Enterprise GRC 6.1: User's Guide*. Cary, NC: SAS Institute Inc.

SAS® Enterprise GRC 6.1: User's Guide

Copyright © 2014, SAS Institute Inc., Cary, NC, USA

All rights reserved. Produced in the United States of America.

For a hardcopy book: No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, or otherwise, without the prior written permission of the publisher, SAS Institute Inc.

For a Web download or e-book: Your use of this publication shall be governed by the terms established by the vendor at the time you acquire this publication.

The scanning, uploading, and distribution of this book via the Internet or any other means without the permission of the publisher is illegal and punishable by law. Please purchase only authorized electronic editions and do not participate in or encourage electronic piracy of copyrighted materials. Your support of others' rights is appreciated.

U.S. Government License Rights; Restricted Rights: Use, duplication, or disclosure of this software and related documentation by the U.S. government is subject to the Agreement with SAS Institute and the restrictions set forth in FAR 52.227–19 Commercial Computer Software–Restricted Rights (June 1987).

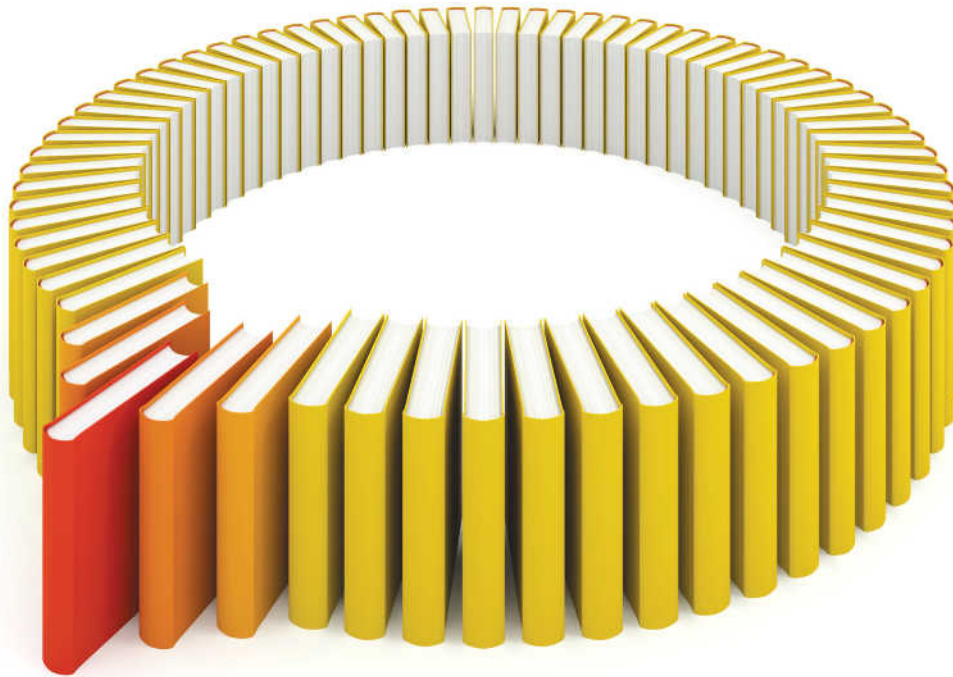
SAS Institute Inc., SAS Campus Drive, Cary, North Carolina 27513.

Electronic book 1, October 2014

SAS® Publishing provides a complete selection of books and electronic products to help customers use SAS software to its fullest potential. For more information about our e-books, e-learning products, CDs, and hard-copy books, visit the SAS Publishing Web site at support.sas.com/publishing or call 1-800-727-3228.

SAS® and all other SAS Institute Inc. product or service names are registered trademarks or trademarks of SAS Institute Inc. in the USA and other countries. ® indicates USA registration.

Other brand and product names are registered trademarks or trademarks of their respective companies.



Gain Greater Insight into Your SAS® Software with SAS Books.

Discover all that you need on your journey to knowledge and empowerment.

 support.sas.com/bookstore
for additional books and resources.


THE POWER TO KNOW.

SAS and all other SAS Institute Inc. product or service names are registered trademarks or trademarks of SAS Institute Inc. in the USA and other countries. ® indicates USA registration. Other brand and product names are trademarks of their respective companies. © 2013 SAS Institute Inc. All rights reserved. S107969US.0613

Contents

<i>About This Book</i>	<i>ix</i>
<i>What's New in SAS Enterprise GRC 6.1</i>	<i>xi</i>
<i>Accessibility Features of SAS Enterprise GRC</i>	<i>xiii</i>
Chapter 1 • Introduction to SAS Enterprise GRC	1
SAS Enterprise GRC Overview	1
Presentation	2
Functionality of SAS Enterprise GRC	2
Risk Management Challenges and SAS Enterprise GRC	4
Chapter 2 • Using SAS Enterprise GRC	7
Overview	7
Logging On	8
Logging Off	8
The SAS Enterprise GRC Home Page	9
Changing User Preferences and Settings	11
Getting Help and More Information	12
Searching for Objects	13
Navigating the User Interface	14
Interacting with SAS Enterprise GRC Records, Dimensional Elements, and Data Objects	23
Chapter 3 • Gathering Governance, Risk, and Compliance Data	27
Overview of Governance, Risk, and Compliance	27
Example of an Entity Implementing SAS Enterprise GRC	28
Defining the Business Structure	30
Defining Users, Roles, and Responsibilities	32
Defining Processes	35
Defining Policies	36
Developing Assessments and Assessment Templates	38
Defining Scenarios	39
Creating Issues and Developing Action Plans	41
Defining Key Risk Indicators	42
Developing Controls and Control Tests	43
Managing Incidents	45
Developing Audits	45
Chapter 4 • Implementing the Business Structure	49
Overview	49
Using the Dimension Browser	50
Mappings	59
Processes	61
Objectives	62
Obligations	63
Chapter 5 • Implementing Users, Roles, and Responsibilities	65
Overview	65
Implementing Users	66
Implementing Roles	66

Example: Assigning a Role and Scope to a User	67
Chapter 6 • Managing Financial Information	69
Overview	69
Overview of Financial Data Menu Options	70
Currencies	70
Exchange Rates	71
Implementing Insurance Policies	72
Chapter 7 • Managing Organizational Policies	77
Overview	77
Policies and Policy Workflows	78
Implementing an Example Policy	81
Chapter 8 • Implementing Issues and Action Plans	87
Overview	87
Implementing Issues and Action Plans	88
Implementing an Example Issue and Action Plan	91
Chapter 9 • Implementing Key Risk Indicators (KRIs) and KRI Workflows	97
Overview	97
KRIs and KRI Workflows	98
Implementing Example KRIs	100
KRI Scoring	106
Chapter 10 • Implementing Controls and Control Tests	111
Overview	111
Controls and Control Testing Workflows	112
Implementing an Example Control Test	115
Chapter 11 • Implementing Audit Missions	123
Overview	123
Audit Missions and Audit Workflows	124
Implementing an Example Audit Mission	127
Chapter 12 • Implementing Scenarios and Scenario Workflows	133
Overview	133
Scenarios and Scenario Workflows	134
Implementing an Example Scenario Assessment	136
Chapter 13 • Managing Risks and Implementing Assessments	143
Overview	144
Assessments and Assessment Workflows	145
Implementing Example Assessment Data Objects	153
Implementing an Example Form-Based Risk Assessment	156
Implementing a Questionnaire-Based Risk Assessment	161
Chapter 14 • Managing Incidents and Incident Workflows	169
Overview	169
Incidents and Incident Workflows	170
Managing an Example Incident	179
Chapter 15 • Viewing Reports	185
Overview of Reports	185
Example: Running a Stored Process Report	188
Example: Creating a Report Using an Information Map in SAS Web Report Studio	189

Example: Launching a SAS Business Intelligence Dashboard	193
Appendix 1 • Performing Other Administrative Tasks	195
Overview	195
Viewing Link Types	196
Managing Screen Definitions	196
Viewing Documentation on Components, Functions, Directives, and Properties	197
Flushing Caches	197
Viewing Configuration Details	197
Managing Locked Objects	198
Viewing Logon Activities	198
Loading, Unloading, and Exporting Data	199
Glossary	205
Index	211

About This Book

Audience

This documentation is intended primarily for users who perform routine data entry and collection tasks by means of the SAS Enterprise GRC Web application. Examples of such users include the following:

- accountants who record loss and event information
- auditors who conduct audits
- control testers who perform tests
- policy administrators who communicate and manage organizational policies
- risk analysts who conduct assessments and monitor key risk indicators in order to evaluate the risk burden of an organization
- risk managers who create and implement action plans for dealing with risk-related organizational issues

Therefore, this documentation assumes a basic knowledge of related risk management goals and terminology. The scope of this guide is primarily limited to tasks that these users are likely to perform. However, many of the initial deployment and implementation tasks that you can perform via the graphical user interface are administrative efforts that might involve system administrators. These tasks are also described in this guide, and include tasks such as loading data, implementing the business structure, and managing workflows.

For more information about installing and configuring SAS Enterprise GRC, see the *SAS Enterprise GRC: Installation and Configuration Guide*.

For more information about administering and customizing SAS Enterprise GRC, see the *SAS Enterprise GRC: Administration and Customization Guide*.

For more information about managing workflows for SAS Enterprise GRC, see the *SAS Enterprise GRC: Workflow Administration Guide*.

What's New in SAS Enterprise GRC 6.1

Overview

In SAS Enterprise GRC 6.1, the following new features and enhancements are available:

- support for integration with SAS Visual Analytics for reporting
- simplified installation
- updates to supporting software

Some of the new features and changes listed are specific to administrators of the SAS Enterprise GRC system and might not have any direct impact on your use of SAS Enterprise GRC.

For a full list of changes from the previous version of SAS Enterprise GRC, see the *SAS Enterprise GRC 5.1: User's Guide, Fifth Edition*.

Support for SAS Visual Analytics

SAS Enterprise GRC 6.1 now integrates with SAS Visual Analytics. Users can now shift between the SAS Enterprise GRC and SAS Visual Analytics user interfaces for managing and running reports.

Simplified Installation

The procedure to install SAS Enterprise GRC and its dependent products has been simplified.

Updates to Supporting Software

SAS Enterprise GRC integrates with several software products and solutions which have been updated for this release, including the following:

- SAS Foundation

xii *What's New in SAS Enterprise GRC 6.1*

- SAS BI Server
- SAS Social Network Analysis Server
- SAS Workflow Studio
- SAS Visual Analytics
- SAS Web Report Studio
- SAS Information Map Studio
- SAS BI Dashboard
- SAS Stored Process Server
- SAS OpRisk VaR

Accessibility Features of SAS Enterprise GRC

Overview

SAS Enterprise GRC includes accessibility and compatibility features that improve the usability of the product for users with disabilities, with exceptions noted below. These features are related to accessibility standards for electronic information technology that were adopted by the U.S. Government under Section 508 of the U.S. Rehabilitation Act of 1973, as amended and recommended by the Worldwide Web Consortium (W3C) Web Accessibility Initiative (WAI).

If you have specific questions about the accessibility of SAS products, send them to accessibility@sas.com or call SAS Technical Support.

Supported Web Browsers

The supported Web browsers for SAS Enterprise GRC are Microsoft Internet Explorer 7 and 8 and Firefox 3.6. For more information about the accessibility features of Internet Explorer or Firefox, see "accessibility" in the documentation for that browser.

Resizing the Date Picker

To increase the font size in your Web browser for pop-ups such as the date picker, you can do the following:

- In Firefox, hold down the CTRL key and choose + +.
- In Internet Explorer, in the browser menu, select **View > Text Size > Larger**.

To use the JAWS screen reader with the date picker, toggle the JAWS virtual cursor (**Insert + Z**) to enable date navigation. When the virtual cursor is off, you can change the focus to different dates by using the arrow keys.

Other Known Accessibility Exceptions

SAS Enterprise GRC has the following additional known accessibility issues:

- The Assessment Planning and Audit Planning windows contain dynamic content that is not accessible to assistive technologies. However, all of the information in this

window has an accessible text equivalent in the Assessments or Audit Missions window, respectively.

- Access to some information requires that screen readers are enabled to read alternate text.
- Screen readers do not announce which input fields are required.
- In some cases, screen readers are not able to correctly identify text as the label of an input field.

Chapter 1

Introduction to SAS Enterprise GRC

SAS Enterprise GRC Overview	1
Presentation	2
Functionality of SAS Enterprise GRC	2
Key Features	2
Supported Data Types	3
Supported Data Sources	4
Risk Management Challenges and SAS Enterprise GRC	4
Business Model	4
Data Quality	4
Access	5
Security	5
Regulatory Compliance	5

SAS Enterprise GRC Overview

SAS Enterprise GRC is a user-friendly, Web-based application that automates the management of governance, risk, and compliance (GRC) data. Specifically, it facilitates the entry, collection, transfer, storage, tracking, and reporting of operational losses, gains, recoveries, and key risk indicators (KRIs) that are drawn from multiple locations across an organization. SAS Enterprise GRC consists of the Web application, the SAS Enterprise GRC Administrative Tools, the SAS Enterprise GRC Server, and the Web Help.

SAS Enterprise GRC can also be used to do the following:

- conduct audits
- manage policies
- conduct risk, control, and impact assessments
- assess scenarios
- test controls
- investigate incidents
- create and track issues and develop action plans

Each of these activities can be tied to other activities in the system. Therefore, SAS Enterprise GRC provides an integrated and centralized framework for collecting, managing, and storing GRC information.

Presentation

Many aspects of the SAS Enterprise GRC user interface can be customized. These include menus, tabs, field names, field contents, and the style sheets that control the general look and feel of the application. For example, SAS Enterprise GRC enables the creation of an unlimited number of custom fields.

SAS Enterprise GRC uses a feature called the Custom Page Builder in many areas of the user interface. The Custom Page Builder enables you to create additional fields, modify and remove existing fields, customize the appearance of fields and other objects, and insert functions to control how and when these objects are displayed on the page. In other windows and wizards of SAS Enterprise GRC that do not support the Custom Page Builder, you can enable some additional fields.

In addition, the permissions of specific users and roles affect which types of records are visible and which functionality is available to them within the user interface. To cover the most salient features of SAS Enterprise GRC, this documentation discusses behaviors that are based on the default configuration and global role permissions. For this reason, your user interface and its behavior might, in some cases, appear to be different from that discussed here.

Functionality of SAS Enterprise GRC

Key Features

SAS Enterprise GRC enables you to perform the following tasks:

- Continually monitor and oversee all relevant GRC information.
- Categorize GRC data into hierarchies.
- Adjust to changes in organizational structure and dynamics.
- Use audit tracking to view the entry and modification dates of data, as well as the reasons for changes.
- Support the following approaches to managing incidents: near miss, loss/profit, and component of credit loss.
- Support the following approaches to assessment management: form-based, questionnaire-based, and direct edit.
- Integrate the following business objects with the SAS Workflow Engine: incidents, form-based assessments, control tests, audit missions, policies, and issues and action plans.
- Provide flexible workflows for the approval and review of other business objects.
- Enable the user to raise issues and action plans for key business objects.
- Provide role-based security along multiple dimensions for all business objects.

- Support loading data from spreadsheet and .csv files in addition to managing data through the user interface.
- Integrate SAS Enterprise GRC output with SAS OpRisk VaR.
- Integrate SAS Enterprise GRC with public operational loss data (SAS OpRisk Global Data).
- Link between users and business objects such as events, issues, risks, and controls, and visualize the relationships between these objects.
- Alert notifications (portal alerts, e-mail messages, SMS messages, and e-mail digests) provide options for responding to changes in the GRC environment.

Supported Data Types

SAS Enterprise GRC is designed to help you collect, manage, and understand the following primary types of data:

- assessment and scenario data, which consists of questionnaires and responses that, for specific organizations and business processes, assess the following:
 - exposure to various categories of risk
 - potential impacts that could result from exposure to a risk
 - quality, effectiveness, and coverage of controls
- audit data, which includes information about the costs and outcomes of objective assessments that track quality and compliance
- issue-related information, which includes descriptions of issues and the action plans that are devised to rectify these issues
- key risk indicators (KRIs), which include the following:
 - raw metrics collected automatically from operational systems
 - regularly collected quantitative measures or their estimates
- operational documents, which include spreadsheets, reports, correspondence, and other relevant, but externally produced, electronic material
- operational loss data, which consists of the following attributes related to operational failures:
 - financial effects that can be allocated to locations within your organization
 - offsetting recoveries
 - possible causes
 - potential nonfinancial impacts
 - allocations
 - incident-related workflow and validation workflow

Operational loss data is required for the following:

- regulatory oversight
- capital requirement calculations
- understanding patterns of failure in the context of other risk-related data
- policy data, which includes objectives, correspondence, and costs associated with the periodic communication and monitoring of organizational policies

Supported Data Sources

SAS Enterprise GRC facilitates the integration and distribution of risk knowledge and incorporates data from a variety of sources. Data can easily be loaded from external systems and from pre-existing databases. In addition, data can be entered directly by means of the user interface, or included as attachments. After data has been added to SAS Enterprise GRC, it persists in a transactional system. Thus, data from a variety of sources can be made available for reporting and analysis.

Risk Management Challenges and SAS Enterprise GRC

Business Model

A great challenge of risk management is to correctly situate risk-related data within an organization. Simplistic models of business structure can lead to serious problems in managing risk.

SAS Enterprise GRC models the multidimensional complexity of a real organization in terms of these three organizational spaces:

- structural space, which includes reporting structure, legal structure, business lines, cost centers, and geographies
- operational space, which includes business processes, resources, and products
- risk-analysis space, which includes categories of risks or events, causes, and controls

Moreover, SAS Enterprise GRC models the matrix of relationships among these spaces.

Within this robust framework, SAS Enterprise GRC enables the association of related data. For example, by linking policies with key risk indicators, decision makers and other interested parties can track the effectiveness of the organization in reducing risk by implementing policies. The process of data collection is integrated with a role-based security model so that only those roles with the correct privileges within a specific location can be assigned a given task. As a result, the correct data for each aspect of the business can be collected from the correct people.

Data Quality

The quality of the data in an organization is important to properly understand and manage risk. Poor data quality can limit your ability to manage risk, leading to gaps in controls, flawed decision making, and greater losses. SAS Enterprise GRC maintains data quality in a variety of ways.

- Automatic consistency checks are implemented to guarantee the basic integrity of all the data that has been recorded.
- The structural relationships and referential data about an organization are used to streamline the data-entry process. Users are guided automatically toward valid and relevant content.
- Validation and approval processes ensure that all data has been reviewed and approved by people in the appropriate management or audit hierarchies. Default

workflows provide a template, and existing workflows can be tailored to fit the processes of an organization.

Access

The creation of a risk-aware culture is one of the prerequisites for successful risk management. Such a culture requires that the tools for collecting and managing risk data be available. These tools must be in the hands of employees in each department, at all locations within an organization, and at all times.

For this reason, SAS Enterprise GRC has a variety of attributes that make it accessible to a wide range of users. The Web-based user interface can be used by anyone with access to a Web browser. Users can be notified by e-mail when there are tasks for them to complete or items for them to review. In addition, the simple task-list starting point enables even infrequent users to easily locate tasks that require completion. Finally, SAS Enterprise GRC is scalable, so large numbers of users can use the system.

Security

The security of GRC data is extremely important. This data often includes confidential information about risk exposures and loss incidents that should not be seen by unauthorized users. SAS Enterprise GRC provides a high level of security but does not preclude broad access.

SAS Enterprise GRC uses a simple but powerful role-based security framework. In that framework, meaningful business roles can be defined as needed, given specific privileges and responsibilities, and assigned to users at any combination of points in the organizational space.

Moreover, this framework enables you to do the following tasks:

- Delegate managerial and administrative responsibilities to restricted subsets, such as divisions or departments, of an organization. Such delegation can ease the burden of centralized administration in a controlled way.
- Create confidentiality settings for all data, so that sensitive data can be accessed only by users who have the appropriate security clearance.
- Integrate SAS Enterprise GRC with standard corporate authentication systems, such as LDAP directories and Microsoft Active Directory.
- Create security reports that detail the roles and capabilities of users, and provide a history of actions taken.

Regulatory Compliance

For many organizations, regulatory compliance is crucial for managing risk and for maintaining a good business standing with local and international legal authorities. Regulatory agreements and legislation outline ways to improve the stability and transparency of organizations and financial systems. The applicable agreements and legislation include the New Basel Accord (Basel II), the Sarbanes-Oxley Act of 2002, Canada's Bill 198, Japan's Financial Instruments and Exchange Law, and the European Union's Solvency II. SAS Enterprise GRC facilitates compliance with such guidelines by enabling organizations to do the following:

- Map internal business structures, processes, and risks to their industry-standard counterparts.

- Examine a history of changes for many data objects, such as losses or assessments. These audit trails make it possible to determine who has made a specific change and when each change was made.
- Associate internal controls with industry-standard financial assertions.
- Create, communicate, and monitor policies to facilitate adherence to regulations and industry standards.
- Audit the organization regularly and objectively to determine regulatory compliance.

Chapter 2

Using SAS Enterprise GRC

Overview	7
Logging On	8
Logging Off	8
The SAS Enterprise GRC Home Page	9
Overview	9
The Delegation Bar	10
Changing User Preferences and Settings	11
The Preferences Window	11
Getting Help and More Information	12
The Help Menu	12
The About SAS Enterprise GRC Window	13
Searching for Objects	13
Navigating the User Interface	14
Menus	14
Icons	15
Table Functions	15
Operational Locations and Domains	16
Views	20
Viewing Linked Objects through the SAS Social Network Analysis Interface	20
Interacting with SAS Enterprise GRC Records, Dimensional Elements, and Data Objects	23
Reference Numbers and IDs	23
Dimensional Elements and Data Objects	23
Confidentiality	25
Automatic Currency Conversion	26

Overview

The intent of this chapter is to provide information about using the SAS Enterprise GRC user interface. It provides information about the following:

- [logging on](#) and [logging off](#)
- [using the Home page on page 9](#)
- [changing user preferences](#)

- [getting help](#)
- [using the search feature](#)
- [navigating the user interface](#)
- [understanding and interacting with SAS Enterprise GRC data](#)

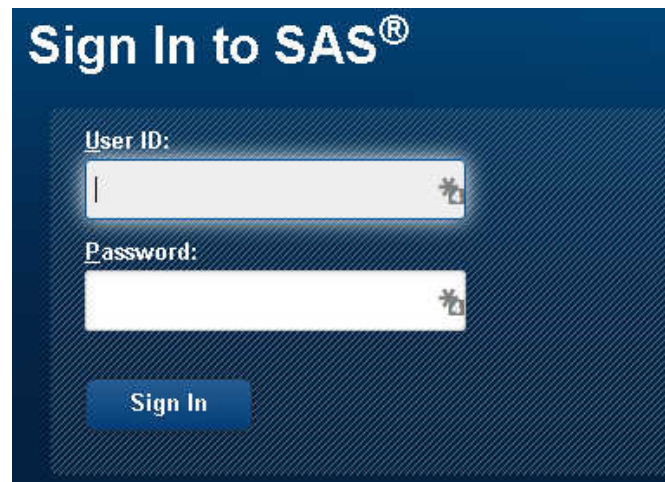
Logging On

SAS Web applications, including SAS Enterprise GRC, use the SAS Logon Manager to enable you to log on to the system. For information about the SAS Logon Manager, see *SAS Intelligence Platform: Security Administration Guide*.

To log on to SAS Enterprise GRC using the SAS Logon Manager:

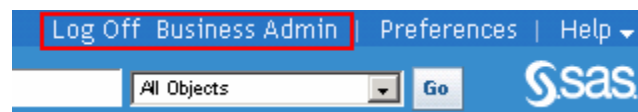
1. Access the SAS Log On dialog box through your Web browser (for example, `http://<Your_Middle_Tier_Host>:8080/SASEnterpriseGRC`).
2. Enter your user name.
3. Enter your password.
4. Click **Log On**.

Display 2.1 Log On Screen

The image shows the SAS login interface. At the top, it says "Sign In to SAS®" in white text on a dark blue background. Below this, there are two input fields: "User ID:" and "Password:". Each field has a small icon of a person and a lock respectively. Below the password field is a blue button labeled "Sign In".

Logging Off

To log off from SAS Enterprise GRC, click **Log Off user name** in the top right corner of your Web browser.



You are returned to the SAS Logon Manager.

Note: If you are simultaneously logged on to multiple windows of SAS Enterprise GRC (this could occur if you open multiple e-mail alert notifications), you should ensure you have logged off and closed each opened window, for security purposes.

The SAS Enterprise GRC Home Page

Overview

After you log in to SAS Enterprise GRC, the Home page typically appears. The following is an example of the Home page.

SAS Enterprise GRC • Home Object ID: [] All Objects [] Go [sas]

Home Incidents Risk Management Scenarios Control Testing Audits Policies KRI Issues and Action Plans Administration Reports

Manage Delegates... Act on behalf of: [myself]

Expand All Sections

Task List Type: <all> Status: <all>

	Type	Activity	ID	Title	Status	Due Date
1	Assessment	Assess	JBS_T003	Migration_CTRL_ASE_T003	Assess	Dec 23, 2010
2	Assessment	Validate Assessment Results	JBS_T005	Migration_CTRL_VAR_T005	Validate Assessment	Dec 23, 2010
3	Assessment	Plan Assessment	JBS_T001	Migration_RISK_PLN_T001	Plan	Dec 23, 2010
4	Assessment	Validate Assessment Results	JBS_T008	Migration_RISK_4ResponseTypes_T008	Validate Assessment	Dec 23, 2010
5	Assessment	Accept-Respond	JBS_T004	Migration_RISK_ARD_T004	Accept/Respond	Dec 23, 2010
6	Assessment	Plan Assessment	JBS_T006	Migration_RISK_Invalidated_T006	Plan	Dec 23, 2010
7	Assessment	Validate Assessment Plan	JBS_T002	Migration_BOTH_VAL_T002	Validate Plan	Dec 23, 2010
8	Assessment	Assess	JBS_T007	Migration_RISK_PartialSignOff_T007	Assess	Dec 23, 2010
9	Audit Mission	Edit Audit Mission	JBS_AM-009	JBS_Data APPROVED Audit Mission #009	Created	Oct 9, 2011
10	Control	Edit Approved Control	JBS_CI-008	JBS_Data Control #008	Approved	

Rows 1 to 10 of 71

Shortcuts

Task Edit Shortcuts...

- Create Action Plan
- Create Assessment Template
- Create Audit Mission
- Create Control
- Create Direct Recovery
- Create Financial Effect
- Create Form-Based Assessment
- Create Incident

Dashboard

risk_indicator_dashboard

risk_indicator

No. of Risks with 01. No External Media Coverage 1 trend=0	No. of Risks with 01. No External Media Coverage 2 trend=0	No. of Risks with Severity 1 trend=1
[Gauge]	[Gauge]	[Gauge]

Links

Links Add Link...

Link Name	Edit	Remove
No data to display.		

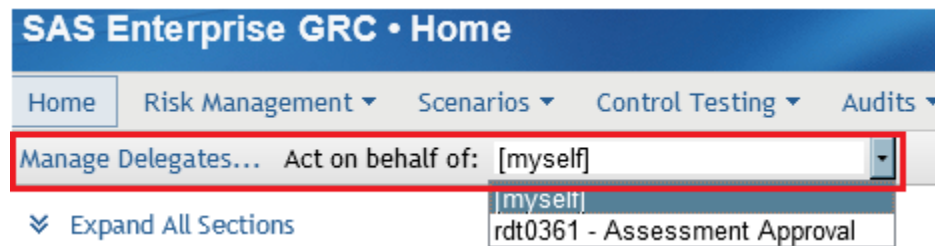
The Home page contains several customizable elements and panels. By default, this consists of the following:

- a delegation bar
- a task list panel
- a shortcut panel
- a dashboard panel (this object is not enabled by default)
- a links panel

Additional information about the delegation bar is provided in the following section.

The Delegation Bar

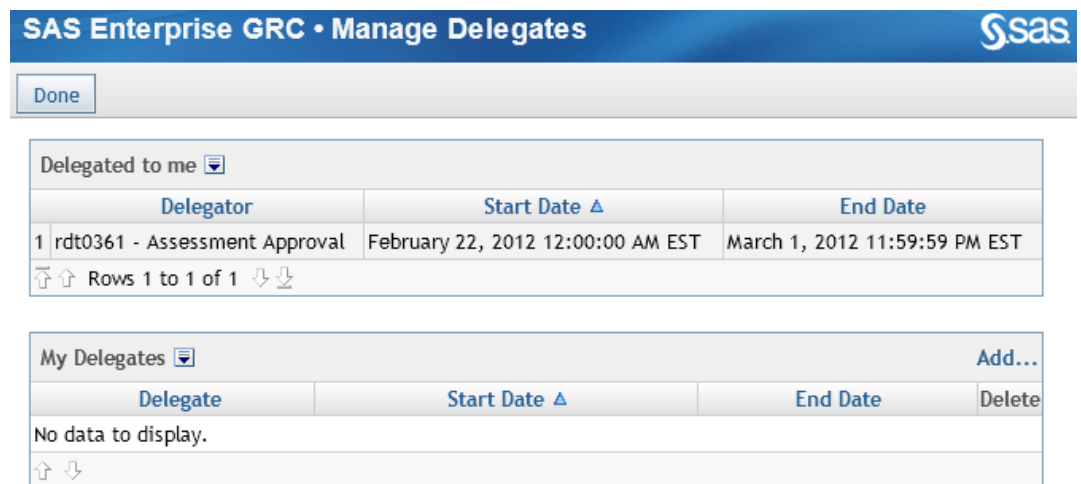
Delegation is the process by which a user can reassign tasks to another authorized user for a defined period of time. The **Delegation** bar enables you to manage your delegates and view tasks that have been delegated to you.



To act on behalf of someone who has delegated their tasks to you, select an option from the **Act on behalf of** drop-down list. This list only appears if someone has delegated their tasks to you.

Note: You must have the same set of roles and the same scope for those roles in order to act on behalf of the person who has delegated their tasks to you.


To manage delegates, click **Manage Delegates**. The Manage Delegates window appears.





The **Delegated to me** table displays the users who have delegated their tasks to you, and provides the start and end dates for the delegation period. This table is read-only.

The **My Delegates** table displays the users that you can select for delegation. To add a delegate, click **Add**. The **Add Delegate** pop-up window appears.


Add Delegate

* **Delegate:** 

* **Start Date:**  (mm/dd/yyyy)

* **End Date:**  (mm/dd/yyyy)

To add a delegate:

1. Click the select user icon () to select a delegate.

Note: To delegate a role, you must select a user that has the exact same roles and scope as you. If you select a user who does not have the same roles and scope for those roles, delegation will proceed, but the delegate will not be able to view or complete any of the tasks that you have assigned to them.

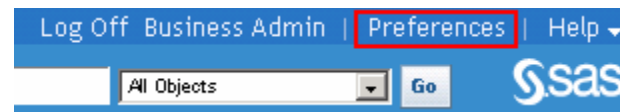
2. Select a **Start Date** for delegation. Delegation will begin at 12:00 a.m. for the time zone of the person who is delegating the task. For example, if you are in Pacific standard time (PST) and the person that you are delegating to is in eastern standard time (EST), delegation will occur at 12:00 a.m. PST, or 3:00 a.m. EST.
3. Select an **End Date** for delegation. Delegation will end at 11:59 p.m. for the time zone of the person who is delegating the task.
4. Click **OK** to save the delegation.

After you have selected a delegate, you can click on the applicable row to edit the delegation and make changes.

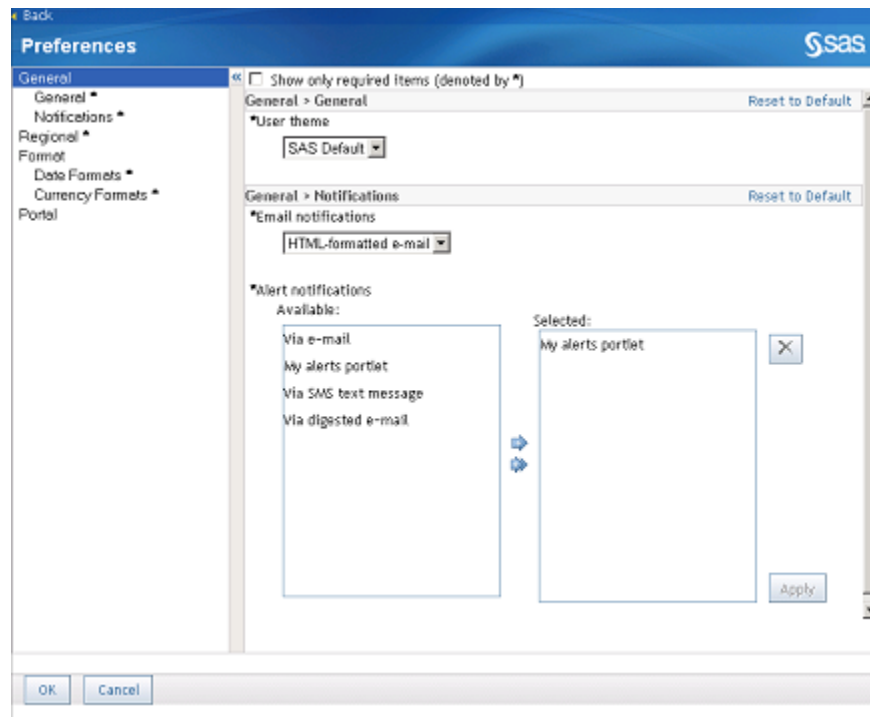
Changing User Preferences and Settings

The Preferences Window

Use the **Preferences** window to change your user preferences and other settings. To access the **Preferences** window, click **Preferences** in the top right corner of your Web browser.

Display 2.2 Preferences Menu Option

The **Preferences** window has four main pages: **General**, **Regional**, **Format**, and **Portal**.

Display 2.3 Preferences Window with Tab Options

- To modify the user theme and the form of e-mail and alert notifications, select the **General** page.
- To change your user language locale and time zone, select the **Regional** page.
- To modify date, time, and currency formats, select the **Format** page.
- To modify portal options, select the **Portal** page.

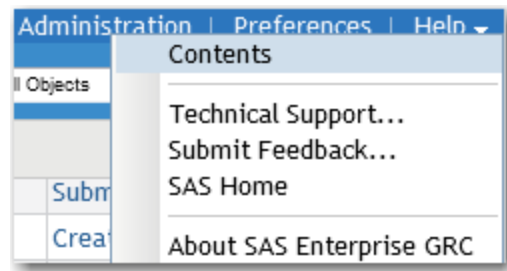
When you have completed your selections on each page, click **OK** to save your selections and return to the main window.

Note: If you modify the language locale settings, you must first log off and then log on to the system for all changes to take effect.

Getting Help and More Information

The Help Menu

Use the **Help** menu to access a variety of help resources. To access the **Help** menu, click **Help** in the top right corner of your Web browser.

Display 2.4 Help Menu Options

- To access online documentation for SAS Enterprise GRC, select **Contents**.
- To access <http://support.sas.com>, select **Technical Support**.
- To submit feedback about SAS Enterprise GRC, select **Submit Feedback**.
- To access the home page of SAS Institute Inc., select **SAS Home**.
- To view details about your installation of SAS Enterprise GRC, select **About SAS Enterprise GRC**. The About SAS Enterprise GRC window appears.

The About SAS Enterprise GRC Window

Use the About SAS Enterprise GRC window to view information about your installation of SAS Enterprise GRC.

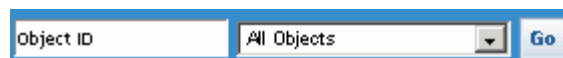
To access the About SAS Enterprise GRC window, click **Help** and select **About SAS Enterprise GRC** from the resulting menu.

The About SAS Enterprise GRC window displays the following information:

- SAS Enterprise GRC release information
- SAS Enterprise GRC copyright information
- Legal Notices
- (Only for users that have the Super-User global capability) Configuration details. For information about configuration details, see [“Viewing Configuration Details” on page 197](#).

Searching for Objects

Use the **Search** widget to find objects. Enter an Object ID and select an Object Type from the drop-down list.



For more information about IDs, see [“Reference Numbers and IDs” on page 23](#).

Navigating the User Interface

Menus

The SAS Enterprise GRC workspace provides a menu bar with the following menus (your ability to access menus and menu items within each menu depends on your permissions):

- The **Home** menu enables you to access the home page and task list.
- The **Incidents** menu contains menu items for creating and investigating incidents and incident-related objects, and for managing validation workflows for incident-related objects. For information about managing incidents, see [“Managing Incidents and Incident Workflows” on page 169](#).
- The **Risk Management** menu contains menu items for identifying risks, causes, potential impacts, and controls, and administering risk and control self-assessments. For information about implementing risks and assessments, see [“Managing Risks and Implementing Assessments” on page 144](#).
- The **Scenarios** menu contains menu items for creating and conducting scenarios. For more information about working with scenarios, see [“Implementing Scenarios and Scenario Workflows” on page 133](#).
- The **Control Testing** menu contains menu items for conducting control tests and creating control certifications. For more information about controls and the control testing process, see [“Implementing Controls and Control Tests” on page 111](#).
- The **Audits** menu contains menu items for planning and conducting audits. For more information about the audit process, see [“Implementing Audit Missions” on page 123](#).
- The **Policies** menu contains menu items for creating, editing, and responding to policies. For more information about managing policies, see [“Managing Organizational Policies” on page 77](#).
- The **KRI** menu contains menu items for managing and collecting KRI (Key Risk Indicator) data. For more information about managing KRIs, see [“Implementing Key Risk Indicators \(KRIs\) and KRI Workflows” on page 97](#).
- The **Issues and Action Plans** menu contains menu items for administering issues and action plans. For more information about managing issues and action plans, see [“Implementing Issues and Action Plans” on page 87](#).
- The **Custom Objects** menu contains menu items for administering additional tasks that you customize. For more information about managing custom objects, see the *SAS Enterprise GRC: Administration and Customization Guide*.
- The **Administration** menu contains menu items for the following:
 - managing user profiles and roles
 - viewing link types
 - managing screen definitions and viewing documentation on components, functions, directives, and properties that are used to customize the user interface
 - performing site maintenance
 - managing the business structure

- managing financial data
- loading and unloading (deactivating) data

See “[Implementing Users, Roles, and Responsibilities](#)” on page 65 for information specific to role and user information. For other administrative work, see “[Performing Other Administrative Tasks](#)” on page 195.

- The **Reports** menu contains menu items for running custom reports. See “[Viewing Reports](#)” on page 185 for more information about viewing reports.

For information about creating and editing reports, see "Reports" in *SAS Enterprise GRC: Help* and the *SAS Enterprise GRC: Administration and Customization Guide*.

Icons

Many windows include icons that enable you to access additional functionality. These icons are displayed in the following table.

Table 2.1 Icons





 Add User	 Assessors/Positions	 Create
 Create Assessment	 Create New From	 Delete
 Edit	 Edit Expression	 Preview
 Remove	 Requires Validation	 Select Date
 Select Insurance Policy; View History	 Select Questionnaire	 Select Ratings Template
 Select User	 View	 Select Measures
 Confidential	 Action	 View Links
 Save	 Export to Excel	



Table Functions


Table functions enable you to view, navigate, sort, and access information throughout tables in the user interface.


For information about using table functions, see "Table Functions" in *SAS Enterprise GRC: Help*. The following figure shows an example of the Measures table.

Display 2.5 Example Table

Measures 										Create Measure...
	Measure ID	Name 	Description	Measure Short Name	Assessable Type	Is Monetary?	Is Default?	Calculation	Default Response Scale	Is Active?
1	IND_1	01. No External Media Coverage	01. No External Media Coverage	IND_1	Risk	No	No		Indirect Effect 1	Yes
2	IND_2	02. Local Media Coverage	02. Local Media Coverage	IND_2	Risk	No	No		Indirect Effect 2	Yes
3	IND_3	03. Regional Media Coverage	03. Regional Media Coverage	IND_3	Risk	No	No		Indirect Effect 3	Yes
4	IND_4	04. National Media Coverage	04. National Media Coverage	IND_4	Risk	No	No		Indirect Effect 1	Yes
5	4	Appetite	Appetite	APT	Risk	Yes	Yes			Yes
6	INH_FI_FRQ2	Calculated Frequency (Inherent)	Calculated Frequency	INH_FI_FRQ2	Risk	No	No	MAX(INH_FI_FRQ, 1)	Calculated Frequency	Yes
7	RES_FI_FRQ2	Calculated Frequency (Residual)	Calculated Frequency	RES_FI_FRQ2	Risk	No	No	MAX(RES_FI_FRQ, 1)	Calculated Frequency	Yes
8	ADE	Control Adequacy	Control Adequacy	ADE	Control	No	Yes		Control Adequacy	Yes
9	DEMOCONTROL_DESIGN	Control Design Rating	Control Design Rating	DEMOCONTROL_DESIGN	Control	No	No		Control Design Scale	Yes
10	EFF	Control Effectiveness	Control Effectiveness	EFF	Control	No	Yes		Control Effectiveness	Yes

 Rows 1 to 10 of 75 

At the top of the table, the down arrow () enables you to choose to customize, search, or export the table, as well as view table customization information.

The Ascending Sort icon () next to the Name label indicates that the table is sorted by Name in ascending order. The Table Status bar at the bottom of the table indicates that rows 21 to 30 are displayed and that the entire table contains 82 records. The navigation icons that enable you to page through rows of data are also displayed at the bottom of the table.

Operational Locations and Domains

Operational Location and Domain Overview

For the purpose of risk management, you associate objects with locations in your organization. In this context, the location of an object is referred to as its operational location (OL). This operational location can be a single point in the dimensional space of your organization, which is defined as the intersection of different dimensions. It can also be a larger operational area that is defined by several operational points. Thus, an operational point is a subset, or a special case, of an operational area.

In the case of incidents, operational locations are referred to as *domains*.

Using the OL Chooser

The operational location (OL) chooser is a common user interface component that enables you to associate each data object with a specific operational location. For example, you might want to associate a specific loss with the organizational point that is represented by the combination of a management organization and a legal organization. Alternatively, you might want to create an action plan that addresses an operational area that is spanned by two geographies and a specific product.

In addition, SAS Enterprise GRC enables you to filter the data objects that you want to view based on the part of your organization to which they are relevant. For example, you might want to view all events of a specific risk event type or all key risk indicators that apply to a collection of causes.

Similarly, the operational locations that you associate with a user through roles define the scope of that user's permissions. For example, you might want to give a central risk manager permissions to conduct assessments in two different management organizations. This framework provides great flexibility for assigning permissions that are appropriately targeted to the responsibilities of different individuals within your organization.

In addition, you can configure how users are able to use the OL chooser to select an operational location. You can specify the following:

- the [mode](#) of the OL chooser
- the default operational location of the user (used when creating some objects)
- which dimensions are allowed or required when users select an operational location
- whether users can select multiple dimensional elements that are in a single dimension
- whether users can select any node or only leaf nodes

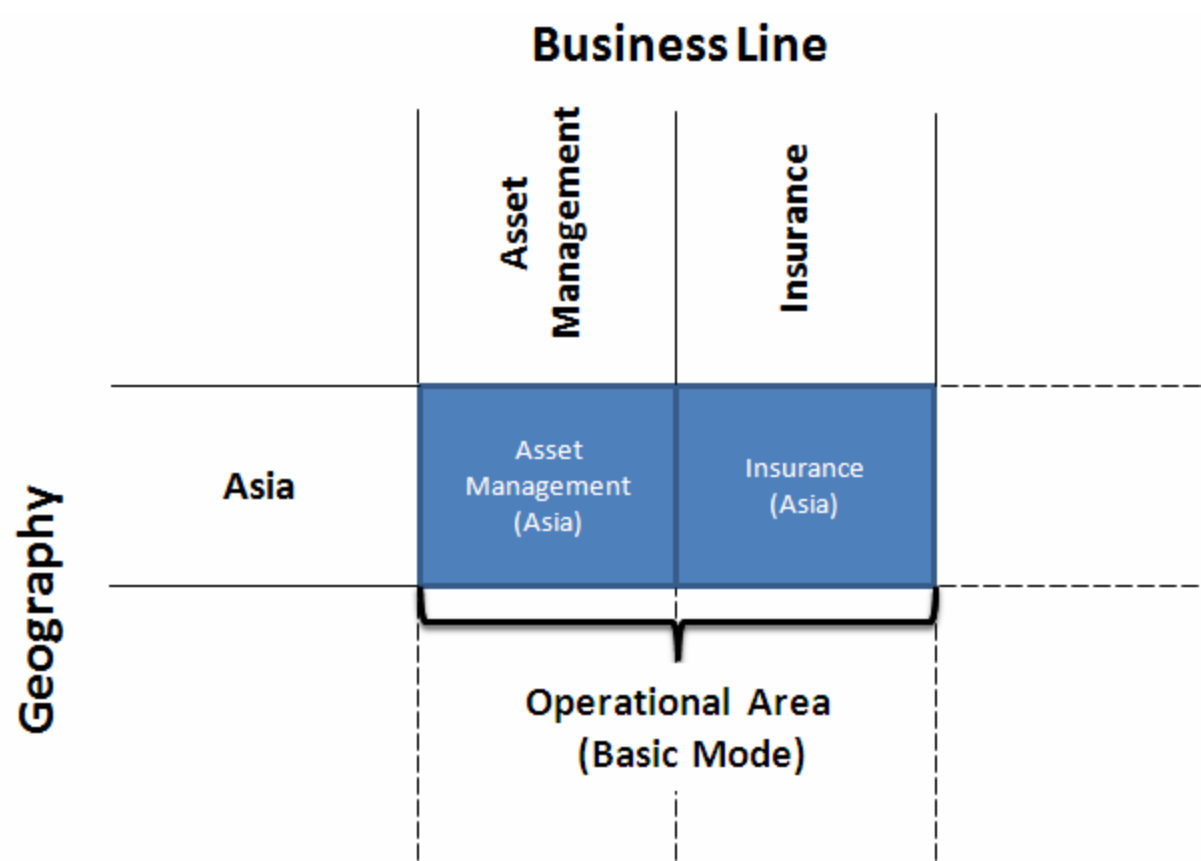
For information about how to configure these aspects of the OL chooser, see the *SAS Enterprise GRC: Administration and Customization Guide*.

The Two Modes of the OL Chooser

The OL chooser has two modes: a Basic mode and a Collection-of-Points mode. You can choose which mode to use by changing your configuration of SAS Enterprise GRC or, in some configurations, by making an appropriate selection in the user interface. The default configuration provides the OL chooser in Collection-of-Points mode for issues, action plans, key risk indicators, nonfinancial effects, and user positions. It provides the OL chooser in Basic mode for all other objects.

When the OL chooser is in Basic mode, much of the process of selecting an operational location is automated. The OL chooser assumes, from your choices of dimensional elements, which operational points should be used to determine an operational area. For example, you might select the two business lines **iFinance > Asset Management** and **iFinance > Insurance** and the geography **Asia**. Then the OL chooser in Basic mode would assume that you want to select the two operational points **iFinance > Asset Management, Asia** and **iFinance > Insurance, Asia**. These two points together define an operational area for Asia that spans these two business lines. The following figure shows how this area is defined.

Display 2.6 Basic Mode



The following figure shows how this operational area is displayed in the user interface.

Display 2.7 OL Chooser, Basic Mode

* Operational Area

Edit | Clear | Favorites▼

* Management Organization:

iFinance > Asset Management

iFinance > Insurance

* Geography:

Asia





In contrast, when in Collection-of-Points mode, the OL chooser enables you to specify a collection of operational points directly. In that case, you can manually determine the operational area that is selected. For example, suppose that you select the two business lines **iFinance > Asset Management** and **iFinance > Insurance** and the geography **Asia**. However, suppose that you choose to restrict only the second business line by means of this geography. In this case, the selected operational area spans the area that is defined by the two operational points **iFinance > Asset Management** and **iFinance > Insurance, Asia**. This operational area is larger than that spanned by the two operational points **iFinance > Asset Management, Asia** and **iFinance > Insurance, Asia** because it does not exclude **iFinance > Asset Management** objects that are located outside of Asia. The following figure shows how this area is defined from a collection of points.

Display 2.8 Collection of Points Mode

		Business Line	
		Asset Management	Insurance
Geography	Asia	Asset Management (Asia)	Insurance (Asia)
	EMEA	Asset Management (EMEA)	
	Americas	Asset Management (Americas)	

The following figure shows how this operational area is displayed in the user interface.

Display 2.9 OL Chooser, Collection-of-Points Mode

* Operational Area		New Point... Clear Favorites▼
Points		Actions
* Management Organization: iFinance > Asset Management		 
* Management Organization: iFinance > Insurance Geography: Asia		 


Filtering Displayed Objects Using the OL Chooser

In many windows in SAS Enterprise GRC, the operational location that is selected determines which items are displayed. Only those items that are located at or within the selected location and that the user has the appropriate permissions to view are displayed. For example, if you want to view only those issues in the Issues window that are associated with the Americas, then you can use the OL chooser to select the geography

Americas. The Issues table then refreshes and displays the relevant issues for that geography. If you want to view all issues, regardless of their locations, then you can clear the selected operational location by clicking **Clear**.



Views

In many windows in SAS Enterprise GRC, a view bar enables you to customize and save a table view and perform additional actions on the view. A table view can capture a combination of OL chooser filters and table functions.


On the view bar, the Menu action button () enables you to save or delete a view, and to customize, search, or export the table. Any searches or customizations to the table can be saved in a table view.

For example, you might have a role in which you investigate active incidents for the iFinance business line for the Americas geography. You want to view only active incidents that fit the criteria of the filter, and you want to sort by event ID.

To configure this view:

1. From the menu, select **Incidents > Incidents**.
2. In the OL chooser, do the following:
 - a. Click **Edit**. The Operational Area chooser window appears.
 - b. In the Operational Area window, add **iFinance** for the Management Organization dimension and add **Americas** for the Geography dimension, and click **OK**.
3. On the Incidents view bar, click the Menu action button () and select **Search**. The Generate Query window appears.
4. In the Generate Query window, do the following:
 - a. Select **Is Active?** for the **Column**.
 - b. Select **Is Equal To** for the **Condition**.
 - c. Select **Yes** for the **Value**.
 - d. Click **Add** to add the expression to the filter. Click **OK** to close the Generate Query window.
5. Click the **Event ID** label in the table to sort by Event ID.
6. On the Incidents view bar, click the Menu action button () and select **Save View**. Enter *Active Incidents* as the **Name** and click **OK**.

To make a view for a particular window your default view, click the **Set as default view** option on the view bar.

To delete a view, click the Menu action button () and select **Delete View**.

Viewing Linked Objects through the SAS Social Network Analysis Interface

To view and explore linked objects through the SAS Social Network Analysis interface, you can click **View Links** from a corresponding window. You can use the social network analysis diagram that appears to graphically view the relationships between objects.

There are two types of nodes, user nodes and business object nodes. A user node refers to a person. A business object node can be any number of different business objects (risks, controls, issues, action plans, incidents, and so on).

To view or make annotations about a node, you can click **Annotate** when your pointer rests on a node.

Note: HTML tags are displayed when you select **Annotate**. If you do not want to see the HTML tags along with the annotations, do not include any HTML tags in the annotation.



The following table displays the objects that are supported for this interface:















Table 2.2 *Business Objects Supported in the Linked Objects Graph Interface*

Action Plans	Allocations	Assessments
Assessment Templates	Audits	Causes
Controls	Control Certifications	Events (Incidents)
Financial Effects	Incident Causes	Incident Controls
Insurance Policies	Issues	KRIs
KRI Definitions	KRI Observations	KRI Observation Requests
Nonfinancial Effects	Objectives	Obligations
Policies	Policy Responses	Potential Impacts
Processes	Questionnaires	Questionnaire Templates
Recoveries	Risks	Scenarios
Tests	Test Definitions	Test Definition Groups
Users	All Dimensions	

The following table displays the buttons available for this interface.

Table 2.3 *Social Network Analysis Diagram Toolbar Buttons*

Button	Name	Use and Description
	Save Network	Saves the current social network analysis diagram to the database.
	Open	Selecting the down arrow (▼) next to the Open button displays selections to retrieve the original social network analysis diagram (from the stored process) or the most recently modified social network analysis diagram (from the database).

Button	Name	Use and Description
	Run Layout	Selecting the down arrow (▼) next to the Run Layout button displays selections to enable you to choose a layout to impose on the current social network analysis diagram.
	Add Node	After an existing node is selected, enables you to add a new node.
	Add Link	After two nodes are selected, enables you to add a new link.
	Edit Entity	After an entity is selected, enables you to update the current entity information and specifications.
	Delete Entity	After an eligible entity is selected, enables you to delete the entity from the network view.
	Group Nodes	After eligible nodes are selected, enables you to fold the selected nodes into an individual node that represents the group.
	Regroup Nodes	Enables you to regroup a collection of nodes.
	Collapse Expanded Nodes	Enables you to collapse hidden nodes after they have been expanded.
	Show Map	If enabled for your alert series, displays a map in the background and superimposes all eligible nodes onto the map. See the <i>SAS Social Network Analysis Server: Investigator Guide</i> for details about the map view and node eligibility.
	Hide Map	When the map view is displayed, enables you to hide the map (return to the standard view), while leaving the nodes and links in view.
	Home	Enables you to re-center the social network analysis diagram. In addition, selecting the down arrow (▼) next to the Home button displays options to enable you to pan left, right, up, or down.
	Zoom In	Enables you to zoom in on the social network analysis diagram.
	Zoom Out	Enables you to zoom out of the social network analysis diagram.
	Legend	Opens a legend for node icons and colors. If the solution administrator has not configured the legend, then the Legend window displays, but the Colors tab does not contain legend information for the social network analysis diagram.

By default, the node diagram displays two degrees of linking from the base node. You can expand or collapse the node diagram at different points to explore additional degrees of linking.

In addition, the Linked Objects Graph contains a time and scope controller that enables you to view the evolution of nodes over time, for those networks that contain historical data. The scope controller contains options for viewing the full scope of all relationships as time progresses (**Cumulative**) or to view relationships over time as they begin and end (**Marginal**).

To print, right-click anywhere in the node diagram and then select **Print**. You might need to move the node diagram to the upper left corner and resize it for best results.

To exit the node diagram, click **Close**.

For more information about using the Linked Objects Graph interface, see the *SAS Social Network Analysis Server: Investigator Guide*.

Interacting with SAS Enterprise GRC Records, Dimensional Elements, and Data Objects

Reference Numbers and IDs

Many records in SAS Enterprise GRC have identification attributes, which include *reference numbers* and *IDs*. The following rules apply:

- Reference numbers must be unique for each record regardless of the source system.
Example: Two issues with assigned reference numbers must have unique numbers.
- IDs must be unique for each record that uses the same source system.
Example: Two issues that both have SAS Enterprise GRC as a source system cannot have the same ID.

When you create a new record, the **Reference Number** field and the **ID** field might already be automatically populated. However, in many cases, you can edit these values, provided that they remain unique across all data records. IDs are limited to 32 characters.

Dimensional Elements and Data Objects

Activity Status

All of the dimensional elements in SAS Enterprise GRC have an activity status. The dimensional elements that are displayed in each tree view can be filtered by this activity status. In addition, the actions that you can perform are not constrained by dimensional activity status. For example, you can create assessments for an inactive management organization.

Active, Inactive, and Staged Dimensional Elements

The activity status of a dimensional element is determined by its Active-From and Active-To dates. Dimensional elements are Active during the period from the beginning (first millisecond) of the Active-From date to the beginning of the Active-To date. Otherwise, they are Inactive. Staged dimensional elements are those dimensional elements that are not yet active but will become active at some point in the future. Dimensional elements that are loaded but do not have Active-From and Active-To dates are assumed to have an Active-From date of January 1, 2003, and an Active-To date of

December 31, 9999. The terminal date implies that the dimensional element is active indefinitely.

Activity status is not inherited within a dimensional hierarchy. If a parent dimensional element is inactive, then the descendants of that dimensional element can still be active.

Active and Inactive Data Objects

Some data objects in SAS Enterprise GRC can be active or inactive. These data objects include questionnaire templates, scenario templates, KRI definitions, KRIs, and insurance policies.

The activity status of these data objects influences whether they can be used to create other objects. In general, inactive objects cannot be used to create other objects. For example, a questionnaire template for a specific operational point can be selected for inclusion in an assessment for that operational point only if the template is active. Similarly, an inactive KRI definition cannot be used to create a KRI. Finally, only active insurance policies can be selected for association with a recovery or a response to a risk.

When creating or editing one of these data objects in SAS Enterprise GRC, you are usually given the opportunity to choose whether it is active or inactive. However, questionnaire templates and scenario templates revert to inactive status if they do not contain assessment items.

Editable, Read-Only, and Frozen Data Objects

Data objects in SAS Enterprise GRC can have one of the following properties:

- **editable.** This is a data object that you can edit.
- **read-only.** This is a data object that cannot be changed within a given context. However, changes might be made to the object outside of this context that are visible within the context.
- **frozen.** This is a data object that is read-only. Changes made to it outside a given context are not visible.

For example, if an assessor signs off on a risk, the risk name is frozen for the assessor in the context of the assessment. But if the risk is in the risk profile, then someone can change the risk name outside the context of the assessment. But to the assessor, the risk was frozen in the context of the assessment when they signed off. So viewing the risk inside the assessment displays the name of the risk as it was when the assessor signed off.

Locking and Unlocking Data Objects

Some data objects in SAS Enterprise GRC are locked while they are being edited. When an item is locked, it can be viewed, but not modified, by other users. Moreover, locked data objects are not moved when a dimensional element that contains them is split.

After you lock a data object, it remains locked until you either submit it for validation or approval, or you explicitly unlock it. In addition, items that you are editing can be locked even when you are not logged on to SAS Enterprise GRC. For example, issues, action plans, and questionnaires become locked when you click **Begin Modification** and remain locked until you click **End Modification**.

Incidents become locked when you enter the Investigate Incident Wizard and remain locked until you click **Save** or **Cancel** in that wizard.

The **Locked Objects** window in the **Administration > Site Maintenance** menu enables you to unlock data objects. This feature is useful if users are sharing objects. For example, if you leave the office for a week with an object open for editing, then no other

user can use that object until you return to finish editing the object. This window can be used to unlock the object without having to wait for you to return.

An example locked object is displayed in the following figure. Suppose that another user is editing an issue. This issue is locked and cannot be edited by anyone else. You can unlock the issue using the following steps:

1. Select **Administration > Site Maintenance > Locked Objects** from the menu.
2. Select **Issue** as the **Object Type** and click **Go**.
3. Check the box next to the locked issue.
4. Click **Unlock Selected**.

The following figure shows an example of a locked object in the user interface.

Display 2.10 Example Locked Object

Filter by Operational Area Edit Clear Favorites▼						
Management Organization: (None Selected)						
Locked Objects ▼						Unlock Selected
	Current User	Object ID	Object Last Modified	Name or Title ▲	Current User Last Logged On	Object Last Locked
1	<input type="checkbox"/> rdt0020 - Central Risk Management	10761	April 25, 2014 11:51:03 AM EDT	bw test	April 25, 2014 11:50:53 AM EDT	April 25, 2014 11:51:05 AM EDT
Rows 1 to 1 of 1						

Confidentiality

The administrator can make any number of fields confidential for the following objects:

- Events
- Financial Effects
- Effect Amounts
- Nonfinancial Effects
- Incident Causes
- Incident Failed Controls
- Recovery Amounts



Confidentiality was previously configurable in configdata.properties, but can now be configured via the SAS Management Console. For more information about configuring confidentiality, see the *SAS Enterprise GRC: Administration and Customization Guide*.





If the administrator has not marked any fields as confidential for an object, then you cannot make objects of that type confidential. If the administrator has marked one or more fields as confidential for an object, then you can make objects of that type confidential. If you choose to make an object confidential, then the following fields appear.

Display 2.11 Confidentiality Fields

Confidential: ☒ Yes ☐ No


*** Confidentiality**


Confidential Users 						Add Confidential User...
	User ID	User Name	Default Location	E-mail Address	Title	Remove
1	admin	GRC admin user				

  Rows 1 to 1 of 1  

*** Confidentiality Justification:**

You must take the following actions:

1. Click **Add Confidential User** to add a user to the list of users who can view confidential fields.
2. (Optional) Click the Remove icon  to remove a user from the Confidential Users table.
3. Enter a **Confidentiality Justification**.

If a field has been marked as confidential, then a Confidential icon  is displayed next to that field.

Automatic Currency Conversion

In some windows and wizards, if you enter a monetary value in a particular currency, it is automatically converted to the corresponding amount in the base currency and used to display in a table or populate another field. The conversion uses the exchange rate table to determine the converted values. However, if you do not have currency exchange rates loaded, then the calculated amount in base currency is zero. For more information about currencies and exchange rates, see [Chapter 6, “Managing Financial Information,”](#) on [page 69](#).

Chapter 3

Gathering Governance, Risk, and Compliance Data

Overview of Governance, Risk, and Compliance	27
Example of an Entity Implementing SAS Enterprise GRC	28
Entity Architecture and Dimensionality	28
Defining the Business Structure	30
Overview	30
Management Organization Dimensional Chart	30
Business Line Dimensional Chart	31
Geography Dimensional Chart	31
Defining Users, Roles, and Responsibilities	32
Defining Processes	35
Defining Policies	36
Developing Assessments and Assessment Templates	38
Defining Scenarios	39
Creating Issues and Developing Action Plans	41
Defining Key Risk Indicators	42
Developing Controls and Control Tests	43
Managing Incidents	45
Developing Audits	45

Overview of Governance, Risk, and Compliance

The execution of governance, risk, and compliance (GRC) within an organization requires the successful coordination and completion of a number of management tasks. In order to successfully use SAS Enterprise GRC, you should ensure that many of these tasks are performed before implementation. In addition, some tasks should be performed concurrent with your implementation of SAS Enterprise GRC. This chapter uses the example of an entity, Orion Star, that has established a GRC management framework within its organization, and has launched SAS Enterprise GRC for organizing, managing, monitoring, and auditing GRC activities.

The intent of this chapter is to focus on some of the pre-deployment requirements and to provide an example that can be used as a template in the following chapters for planning, developing, implementing, and maintaining SAS Enterprise GRC within an

organization. Your organization's specific implementation and use of SAS Enterprise GRC depends on a variety of external factors, such as the organization's size, structure, industry type, and the nature of its nonfinancial risk. SAS Enterprise GRC is highly customizable and designed to enable organizations to manage GRC activities across a variety of different infrastructures.

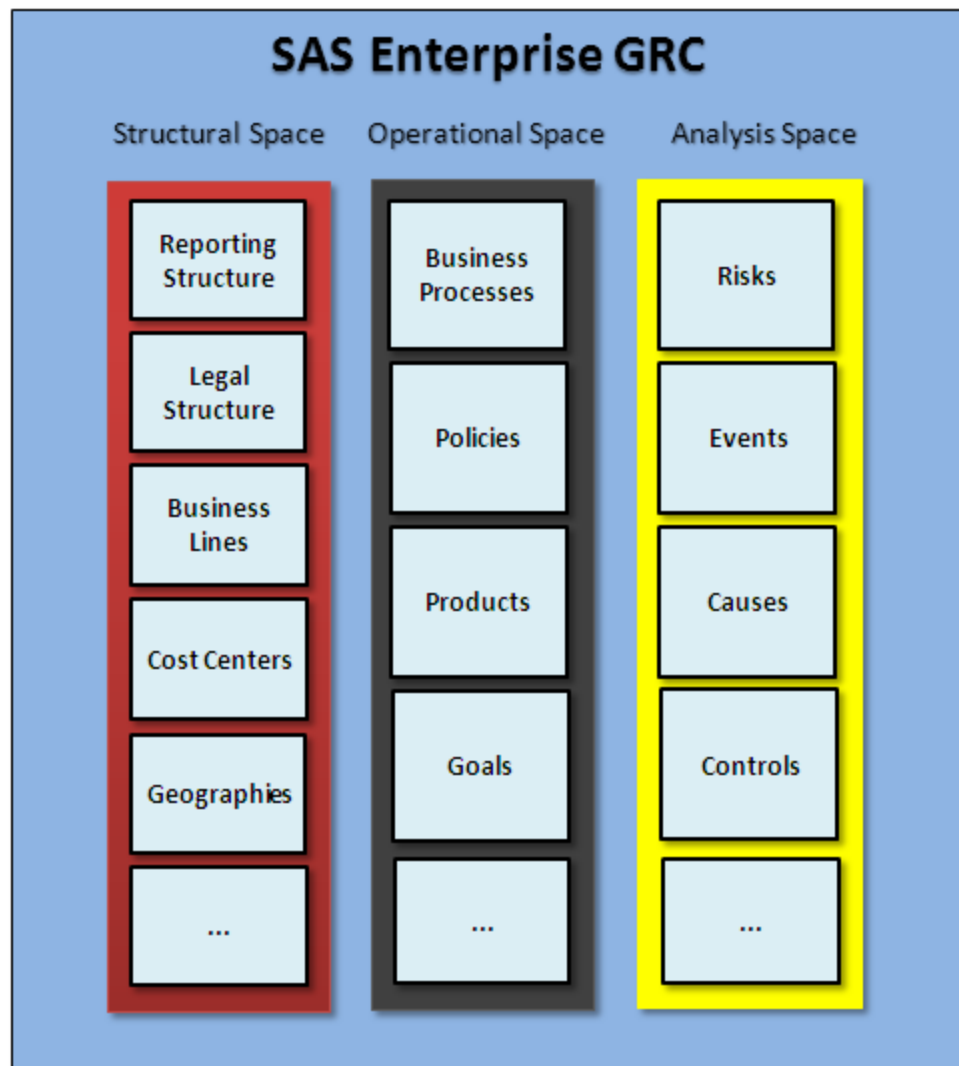
This chapter also provides information about user roles and the standard activities that they perform, so you can understand how each role plays a part in SAS Enterprise GRC.

Example of an Entity Implementing SAS Enterprise GRC

Entity Architecture and Dimensionality

This guide uses the example entity Orion Star, a global bank with more than 25,000 employees, that has developed a management infrastructure for GRC activities. Orion Star is using SAS Enterprise GRC to coordinate, manage, and monitor governance, risk, and compliance activities within its organization. We first define the business architecture of this organization in detail and then explain how it fits into the GRC management framework.

An organization's business is usually a complex environment that consists of many different layers and reporting hierarchies. For example, companies organize themselves by management organization, geography, business line, product line, cost center, and so on. These hierarchies are referred to as the *structural space*. Interwoven in these hierarchies are business processes, policies, products, goals, and so on, which define how the structural space interacts within the environment. These strata are referred to as the *operational space*. Finally, there are risks, events, causes, controls, and other criteria for recognizing and responding to nonfinancial risk. These strata make up the *analysis space*.

Display 3.1 SAS Enterprise GRC Architecture

In SAS Enterprise GRC, these hierarchies and strata are referred to as *dimensions*. Hierarchical elements within each dimension are referred to as *nodes*.

For more information about dimensions, nodes, and dimensionality, see [“Implementing the Business Structure”](#) on page 49.

There are different risks associated with each dimension and node. For example, Orion Star's iFinance organization has an Investment Banking business line that contains a Securities group, which trades in stocks, bonds, and derivatives. Each of these trading departments has different operational risks related to trading.

Another department within the Securities group, Accounting, has responsibilities in reporting the financial results of the Securities group. It has no trading risks, but could suffer losses if an Accounting member is performing fraudulent transactions.

Even within a shared dimension and risk type, there are other cross-dimensions to consider that impact risk and compliance. For example, bond traders in the Securities group might have traders in China and Germany. Differences in infrastructure or controls between these two geographies could impact the frequency and severity of a particular risk type.

These are just a few examples of nonfinancial risks that your organization must define and monitor.

Defining the Business Structure

Overview

Dimensional information about the organization's business structure must be defined within the SAS Enterprise GRC system, in order to use this information for multidimensional reporting and monitoring. This information can be loaded from predefined data sources or can be built using the SAS Enterprise GRC user interface. This section describes three of these hierarchical dimensions that make up the organization's structural space: management organization, business line, and geography.

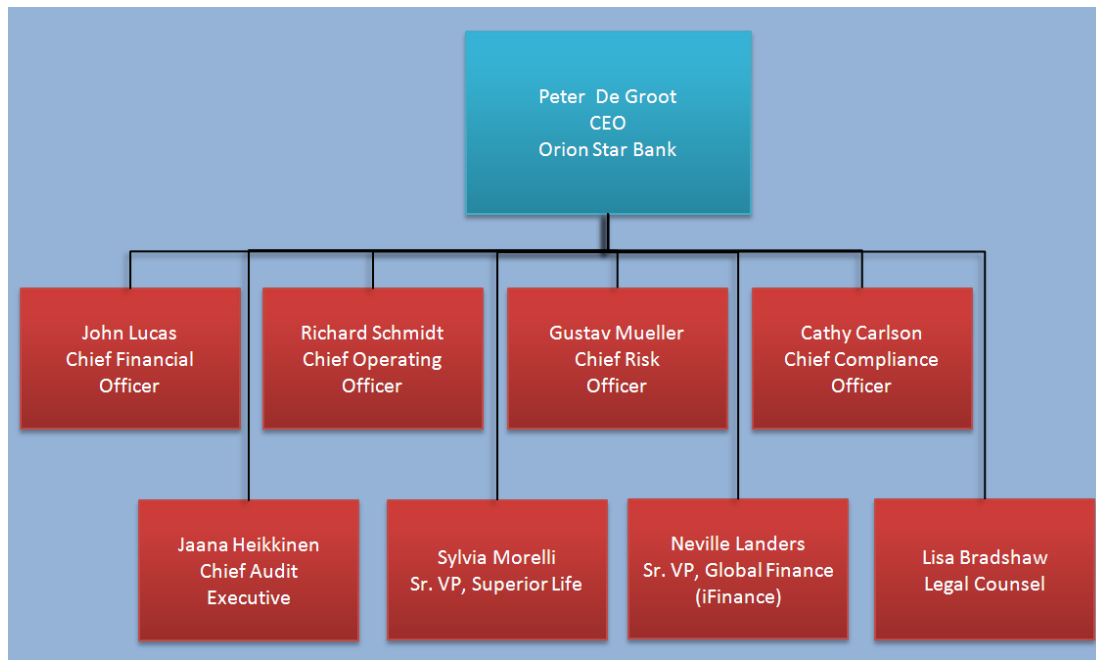
An administrator typically completes the task of loading dimensional information as part of the implementation process. For more information about loading business structure data from other data sources, see the *SAS Enterprise GRC: Administration and Customization Guide*.

For more information about defining the business structure through the SAS Enterprise GRC user interface, see the *SAS Enterprise GRC: Help*.

Management Organization Dimensional Chart

The following management leadership organizational chart is a subset of the entire organizational chart at Orion Star.

Display 3.2 Orion Star's Management Organizational Chart



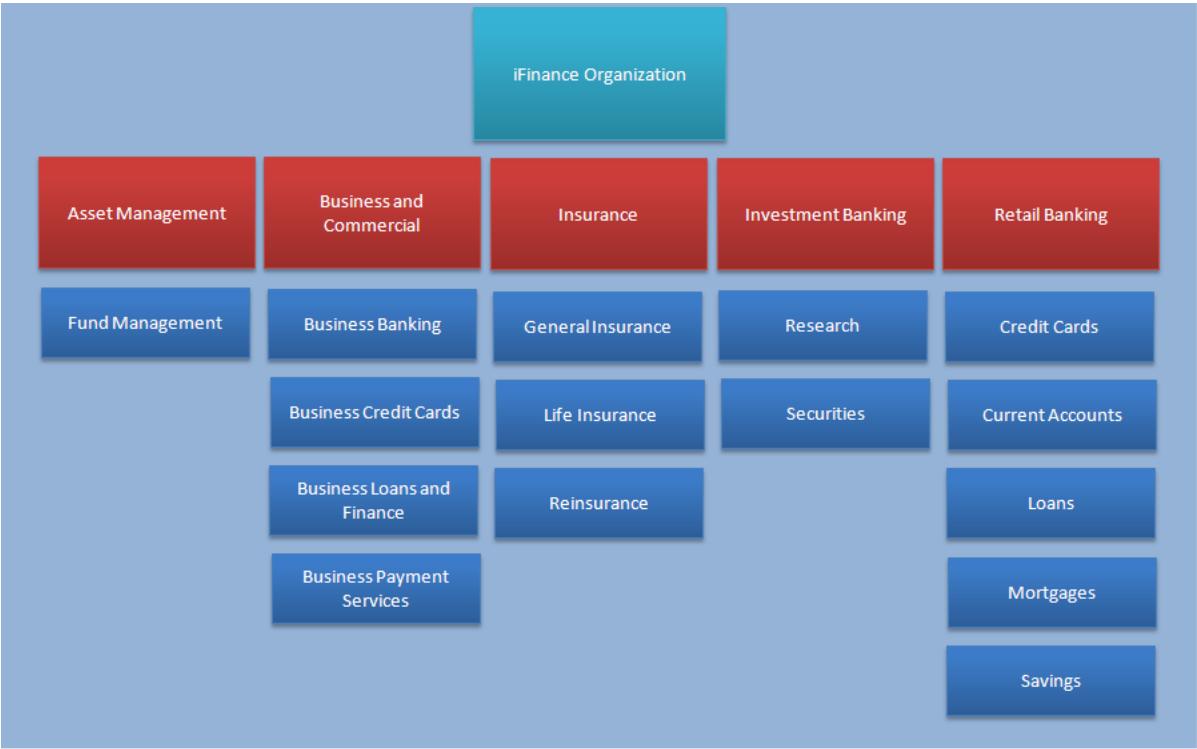
Note: Some dimensional objects might not be required, in this example, for the CEO, CFO, COO, CRO, and CCO positions. However, the iFinance and Superior Life

management organizations each have a number of additional organizations reporting to them. Therefore, they exist in the sample data.

Business Line Dimensional Chart

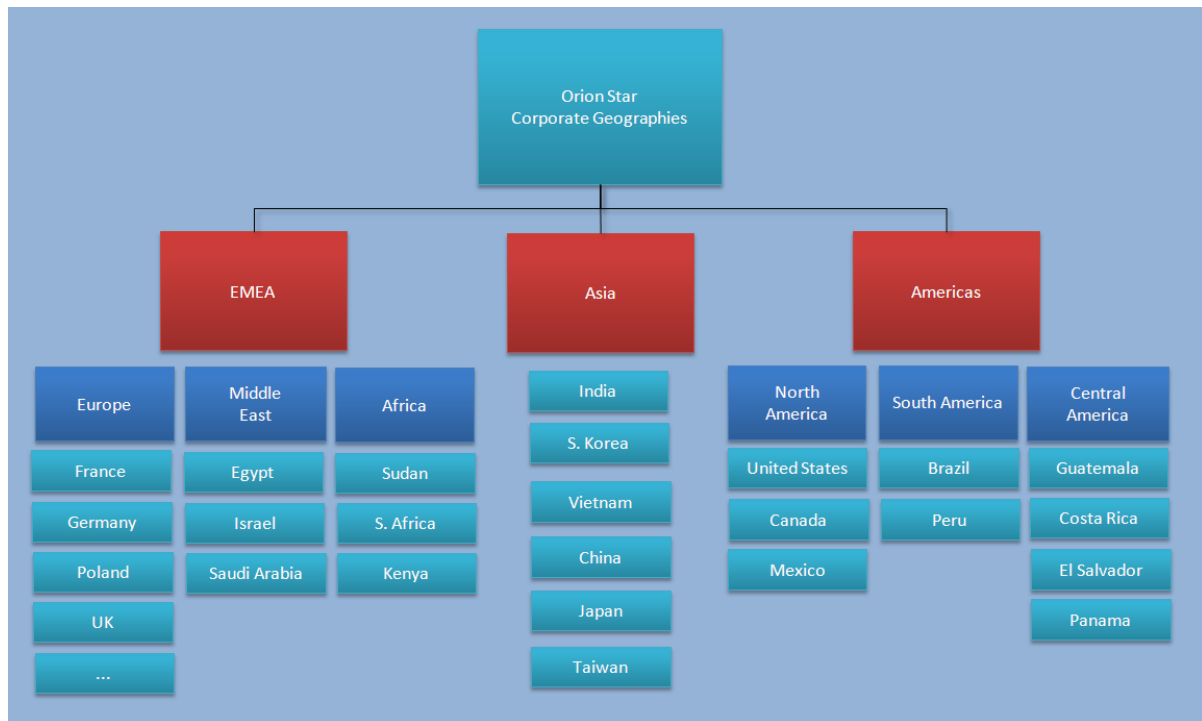
Orion Star has a business line chart that displays its business line dimension. The following chart displays the various business lines under the iFinance organization.

Display 3.3 iFinance Business Lines at Orion Star



Geography Dimensional Chart

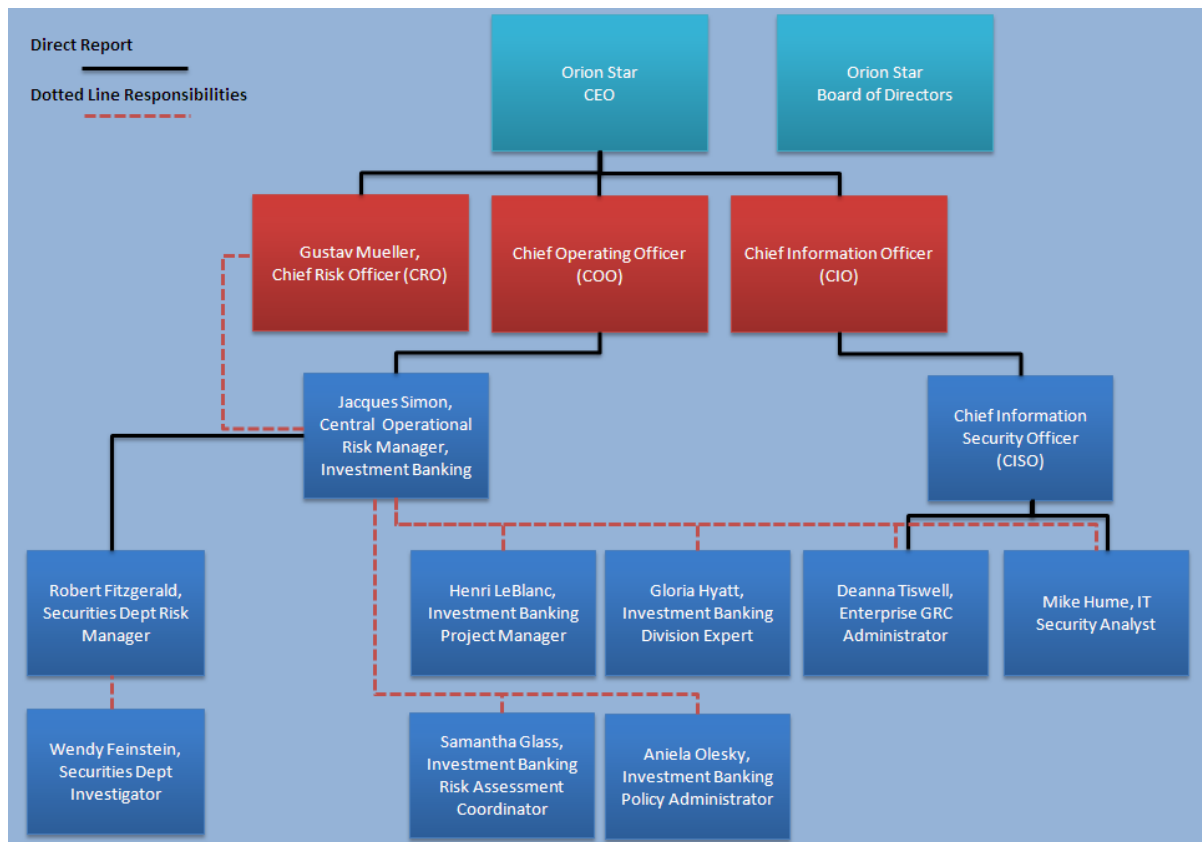
Orion Star has the following geographical dimension to organize its global reporting.

Display 3.4 Geography Chart at Orion Star

Defining Users, Roles, and Responsibilities

Some entities have already started or completed the process of defining roles and responsibilities for users of the system before populating SAS Enterprise GRC with user and role data. Those entities can load this data into the SAS Enterprise GRC system. For an entity that has just begun implementing a GRC infrastructure, all roles and responsibilities related to GRC activities should be understood and clearly defined. This is done through a planning process that gathers organizational data, creates roles, and assigns these roles to people within the organization. In SAS Enterprise GRC, an administrator typically populates users and roles by loading SAS metadata into the SAS Enterprise GRC system through a synchronization process.

For the purposes of understanding the roles needed to carry out these activities, the following organizational chart displays some of the users within Orion Star and their role or roles in its risk management operation.

Display 3.5 Roles and Reporting Responsibilities within the Investment Banking Division of Orion Star

The following table describes a subset of users and their defined roles and responsibilities at Orion Star. In this example, some users have multiple roles and responsibilities.

Note: See “[Developing Audits](#)” on page 45 for a chart of the internal audit group.

Table 3.1 Users, Roles, and Responsibilities at Orion Star

User	Job Title	Responsibility	Enterprise GRC Roles Used for This Example
Gustav Mueller	Chief Risk Officer (CRO), Orion Star	Oversees and sets the strategy for enterprise risk management (ERM) activities at Orion Star. Reports to CEO.	Enterprise GRC: Business Ownership Enterprise GRC: Central Risk Management
Jacques Simon	Central Operational Risk Manager, Investment Banking	Manages and coordinates GRC activities in the Investment Banking Division of Orion Star's iFinance organization. Owns the risk and compliance responsibilities for Investment Banking.	Enterprise GRC: Business Ownership Enterprise GRC: Central Risk Management

User	Job Title	Responsibility	Enterprise GRC Roles Used for This Example
Robert Fitzgerald	Securities Department Risk Manager	Manages compliance and risk in the Securities Department within the Investment Banking Division, and provides management approval for risk activities.	Enterprise GRC: Local Risk Management Enterprise GRC: Local Business Management Enterprise GRC: Allocation Management Approval Enterprise GRC: Recovery Management Approval Enterprise GRC: Incident Management Validation Enterprise GRC: Incident Cause Management Approval Enterprise GRC: Assessment Enterprise GRC: Issue Ownership Enterprise GRC: Insurance Policy Management Enterprise GRC: Control Ownership Enterprise GRC: Test Ownership
Gloria Hyatt	Investment Banking Division Expert	Validates tests, assessments, and incidents across the entire Investment Banking Division.	Enterprise GRC: Assessment Approval Enterprise GRC: Test Definition Approval Enterprise GRC: Allocation Risk Approval Enterprise GRC: Recovery Risk Approval Enterprise GRC: Incident Cause Risk Approval Enterprise GRC: Issue Approval Enterprise GRC: Action Plan Approval Enterprise GRC: Test Results Approval Enterprise GRC: Audit Tests Approval Enterprise GRC: IT Policy Approval
Samantha Glass	Risk Coordinator	Plans and coordinates risk assessments and scenario assessments for the Investment Banking Division. Also plans and coordinates control tests.	Enterprise GRC: Assessment Coordination Enterprise GRC: Test Coordination
Deanna Tiswell	Enterprise GRC Administrator	Administers the SAS Enterprise GRC system and environment. Also administers some risk controls for the Investment Banking Division.	Enterprise GRC: Administration Enterprise GRC: Control Editing

User	Job Title	Responsibility	Enterprise GRC Roles Used for This Example
Mike Hume	IT Security Analyst	Responsible for regularly performing IT control tests for the Investment Banking Division.	Enterprise GRC: Testing
Henri LeBlanc	Risk Project Manager	Responsible for developing programs across the Investment Banking Division to mitigate risk.	Enterprise GRC: Action Plan Ownership
Wendy Feinstein	Securities Department Investigator	Responsible for ensuring the accuracy of financial results. Also investigates financial incidents for issues such as fraud, and certifies controls.	Enterprise GRC: Internal Auditing Enterprise GRC: Incident Investigation Enterprise GRC: Control Certification Ownership
Aniela Olesky	Investment Banking Policy Administrator	Responsible for establishing rules for operating and meeting organizational objectives by managing policies and creating awareness of these policies within the Investment Banking division. Works with upper management, HR, and general counsel to draft and maintain policies.	Enterprise GRC: Policy Administration

This is just one example of users and roles at Orion Star. Your organization might vary in its complexity and scope of responsibility, from a decentralized model, in which many users have only one role, to a highly centralized model where a few users assume many roles. You can customize roles and their assigned capabilities to meet the needs of your organization.

Note: It is recommended that risk managers ensure the segregation of duties. For more information about segregation of duties, see [“Developing Controls and Control Tests” on page 43](#).

An administrator is typically responsible for synchronizing users and roles with SAS metadata, and for assigning users to roles using the SAS Enterprise GRC user interface. For more information about defining users and roles before synchronization with the SAS Enterprise GRC user interface, see the *SAS Enterprise GRC: Administration and Customization Guide*.

For more information about synchronizing users and roles and assigning users to roles using the SAS Enterprise GRC user interface, see [Chapter 5, “Implementing Users, Roles, and Responsibilities,” on page 65](#).

Defining Processes

An important aspect of managing GRC activities is understanding the overall business processes that are involved in performing assessments, creating controls, managing incidents and recoveries, and so on. A central risk manager typically coordinates this effort by aligning corporate ownership with a bottom-up approach that maps out processes and workflow activities for managing and monitoring GRC information. Understanding roles and responsibilities is essential to defining the process components

that are required to attain the desired business objectives. See the subsequent sections in this chapter for examples of workflows that Orion Star uses within its organization.

For more information about customizing GRC processes, see the *SAS Enterprise GRC: Administration and Customization Guide*.

Defining Policies

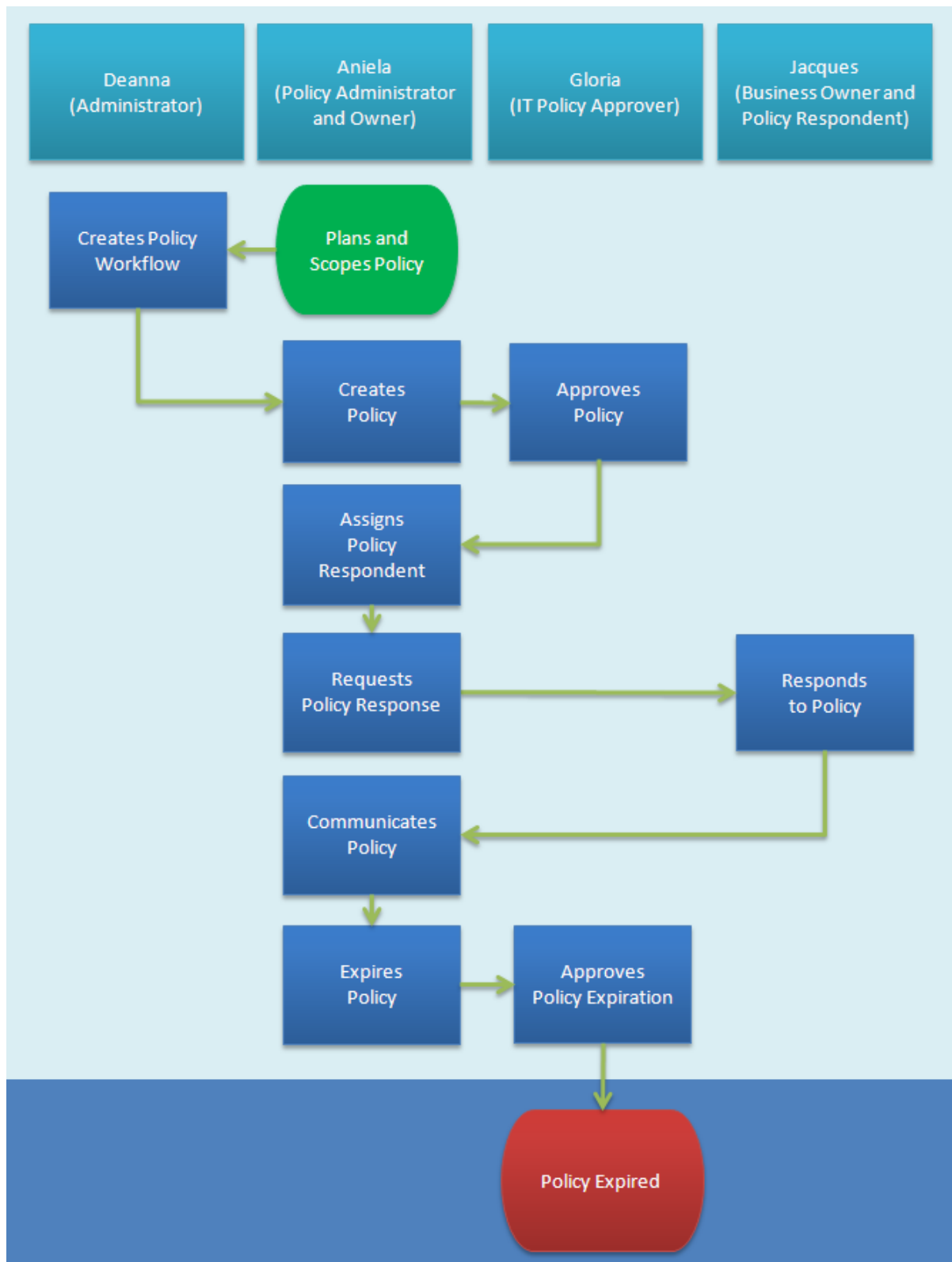
Policies are rules or regulations that govern how an organization achieves its objectives. For example, an organization might have an HR policy that states how employee vacations and personal days are allocated on an annual basis. This HR policy might exist to provide legal protection for the organization, as well as to give employees guidance on how they are to ask for time off and take care of personal matters. Or an IT policy might exist that requires that all users log off from their computers at night, in order to ensure data integrity and protect the organization from security threats.

When a policy is drafted, it might require the acceptance and approval of all parties involved. Some policies might require users to respond to the policy and request exceptions. Over time, these policies might require modification or expiration to account for changes within the organization. The process of maintaining the policy lifecycle is referred to as *policy management*.

Policies can have different workflows, dependent on the type of policy or other customizable criteria. SAS Enterprise GRC uses a highly customizable workflow engine that enables you to design policy management workflows specific to your organization's needs.

Orion Star is using policy management to maintain its corporate policies and ensure that an audit trail exists for the modification and communication of new and existing policies. Specifically, Orion Star has an IT policy that prohibits the use of external e-mail at work. The policy is aimed at reducing Web use and lowering the threat of computer viruses.

The following is an IT policy workflow that was created for the e-mail policy at Orion Star.

Display 3.6 IT Policy Workflow at Orion Star

For more information about managing policies through the SAS Enterprise GRC user interface, see [“Managing Organizational Policies”](#) on page 77.

Developing Assessments and Assessment Templates

The objective of the risk and control assessment process is to collect information about risks, controls, potential impacts, and causes, and to evaluate them. This process involves planning assessments, sending questionnaires to the appropriate people within the organization, and collecting responses. An assessment coordinator is typically responsible for the planning and coordination of risk assessments.

There are two types of process-related risk and control assessments: form-based assessments and questionnaire-based assessments. Both assessments are conducted in stages. Each stage typically requires a validation or sign-off before users can proceed to the subsequent stage. The difference between these two assessment types is in the way that questionnaires are handled. Form-based assessments add questionnaires as file attachments to form an optional pre-assessment that serves to support the assessment. The core assessment is performed at a later stage, using rating templates. Questionnaire-based assessments, however, incorporate questionnaire pages within the user interface to record the risk and control ratings. Form-based assessments are limited to one response form per assessment for all risks and controls, whereas questionnaires can have these items assessed separately.

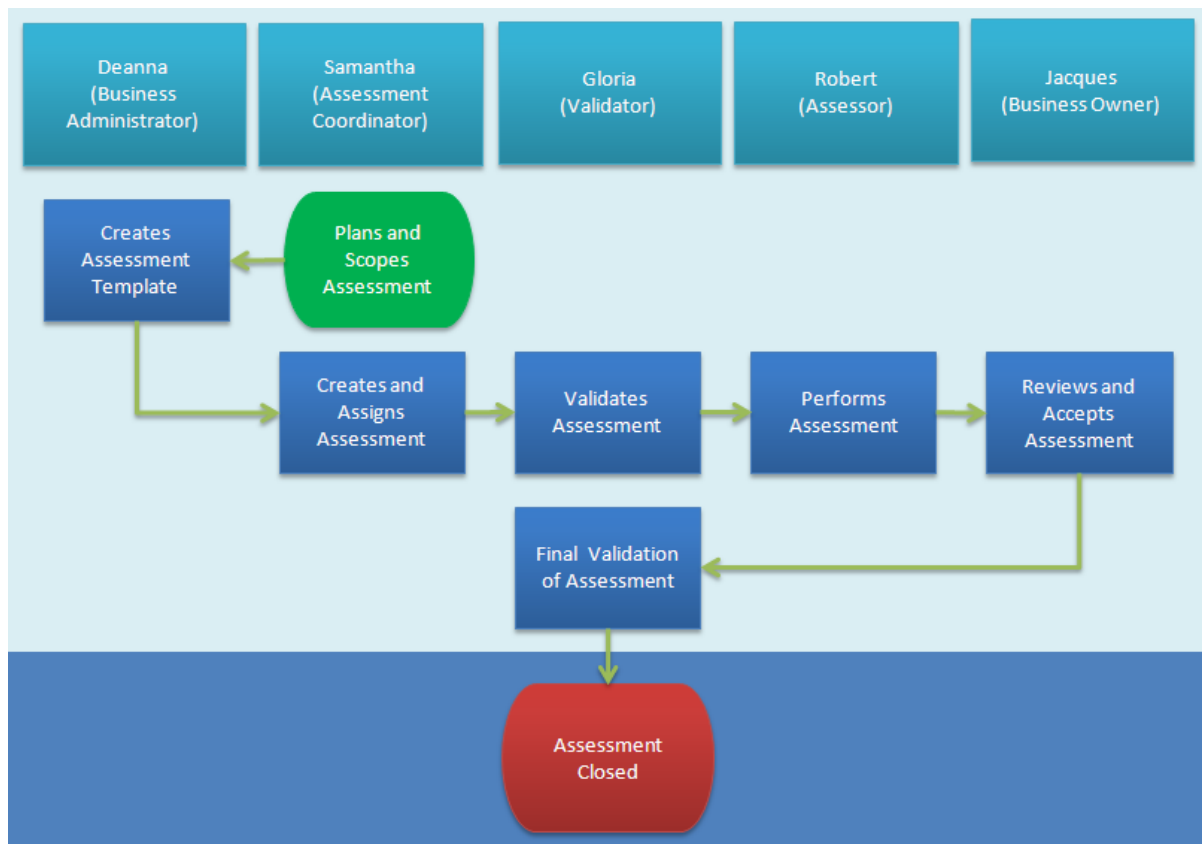
Furthermore, form-based assessments enable the definition of follow-up actions, a management review and response, and automated integration with the issues and action plans.

Whether you conduct a form-based assessment or a questionnaire-based assessment, the assessment process includes a series of reviews and validations that facilitate accountability and create a traceable information stream for auditing and reporting purposes.

A third type of assessment, direct-edit, enables the recording of risk and control ratings directly through the user interface without requiring a validation or sign-off process.

After you have established the business structure, assigned roles, defined risks and risk event types, and defined the necessary workflows and processes for performing assessments, you can create assessments and assessment templates.

Orion Star plans to conduct a quarterly assessment for its Securities department, to assess risks associated with internal fraud at the company. The following is a workflow used by Orion Star to carry out the assessment.

Display 3.7 Form-Based Risk Assessment Workflow for Internal Fraud at Orion Star

For more information about assessment roles and implementing assessments through the SAS Enterprise GRC user interface, see [Chapter 13, “Managing Risks and Implementing Assessments,”](#) on page 143.

Defining Scenarios

In SAS Enterprise GRC, the objectives of the scenario process are to create scenario questionnaires and send them to the appropriate employees so that the expected frequency of future risk events can be assessed for total impact. Scenario topics are created that identify areas that need to be covered for scenario analysis. Scenario templates are created to define the risk event type, the operational area, and the scenario questionnaire. A template can be used for multiple scenarios. Scenarios are then created from these scenario templates and then linked to scenario topics.

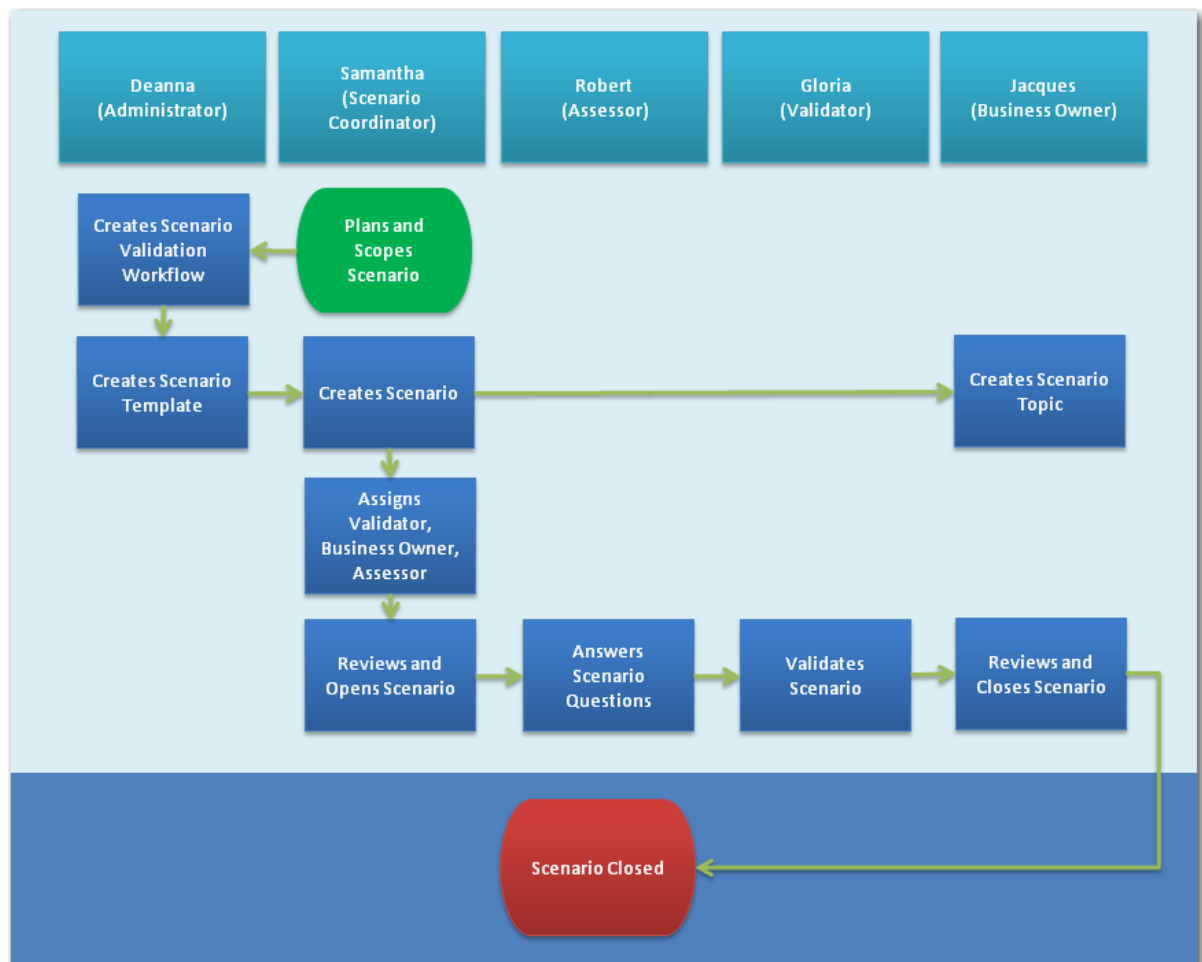
There are two approaches to define scenario templates, bucketed and rare event. A bucketed scenario template asks for the expected frequency of losses for multiple severity ranges. For example, one bucket could have a severity range from \$0 up to \$10,000 in losses and some annual expected frequency of occurrence; another bucket could have a range of \$10,000 to \$50,000 and a different frequency; and a third bucket could range from \$50,000 to \$250,000 and have a third frequency. A rare event scenario is intended to capture information about how often an extreme event happens, and what the expected impact range is. A rare event scenario template also asks only for the minimum severity and maximum severity of an event. The scenario assessor is responsible for filling in this information.

Scenarios are handled in a similar way as risk assessments, in that questionnaires are distributed to employees, information about scenarios is collected, and scenarios are evaluated. As with risk assessments, your organization must first have defined the business structure, assigned roles, defined risks and risk event types, and developed workflows. After you have completed these tasks, you can create scenario templates and scenarios.

After scenarios have been created, you can link scenarios to a scenario topic that you have earlier identified. For example, damage to infrastructure due to natural disaster could be a scenario topic to which multiple scenarios can be linked.

Orion Star plans to conduct a scenario assessment to annually assess potential losses due to unmatched trades and their overall impact on the business, using a bucketed scenario. The following is a scenario workflow used by the Securities department at Orion Star. In this case, roles that perform the risk assessment are also responsible for performing scenario assessments.

Display 3.8 Scenario Workflow at Orion Star for Assessing Fraudulent Transaction Losses



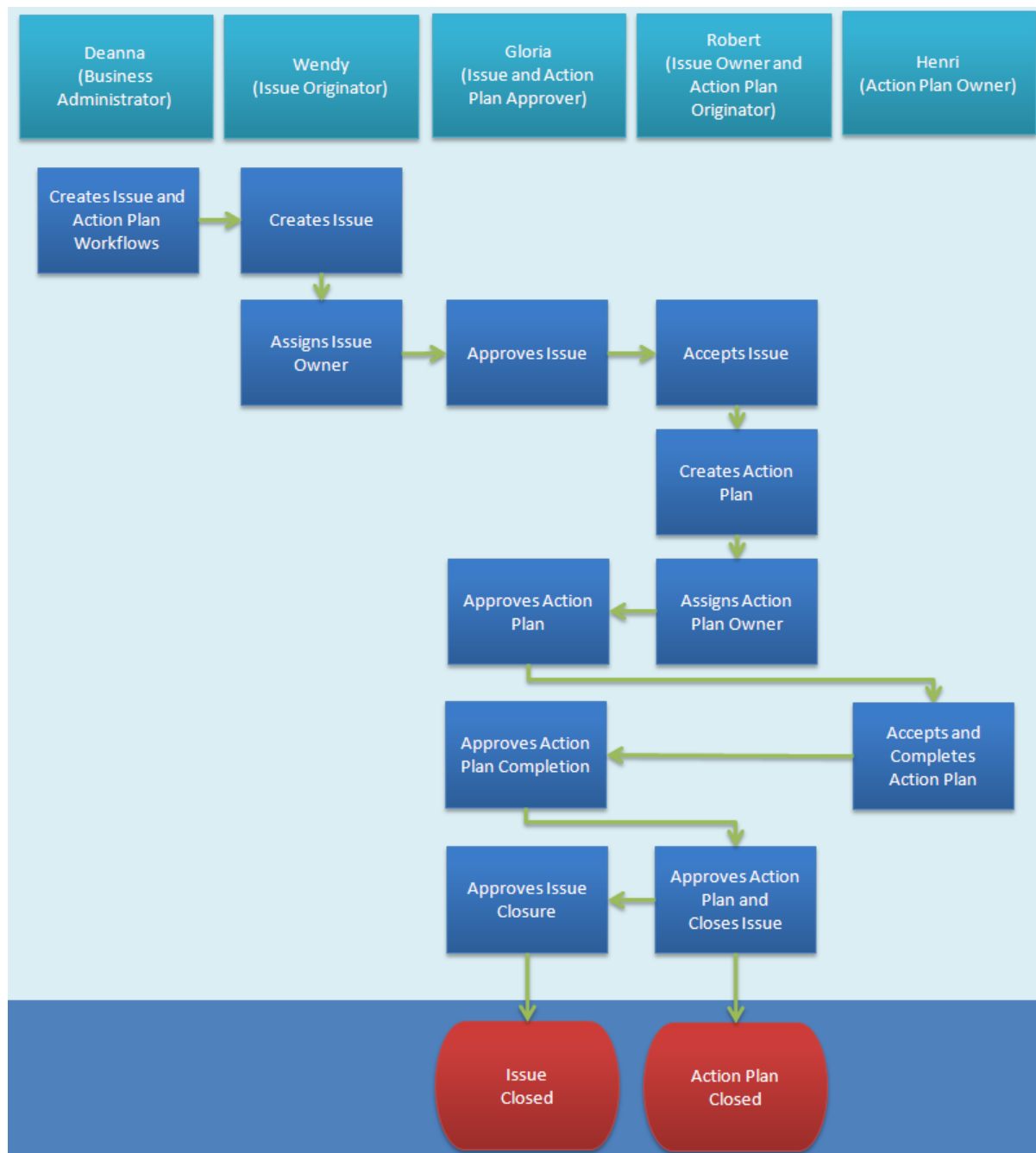
For more information about implementing scenarios through the SAS Enterprise GRC user interface, see [Chapter 12, “Implementing Scenarios and Scenario Workflows,”](#) on [page 133](#).

Creating Issues and Developing Action Plans

In risk management, a *risk* is defined as a potential event that has some impact and a probability of occurring. *Issues*, on the other hand, are gaps or weaknesses in an organization's processes and controls that are identified in the normal course of business. In SAS Enterprise GRC, you can create an issue through the user interface, or the issue can be created automatically through the form-based assessment process or when an incident has breached its issue threshold. This issue threshold depends on the type of risk. For example, one incident might create an issue if a fraud loss exceeds \$10,000. Another issue might be created if there are more than 100 customer complaints made to the customer service desk in a given month. Some incidents might trigger the creation of multiple issues. To address issues, action plans are subsequently created.

Action plans are typically developed in reaction to an issue, but can also be created in response to other events, such as changes in the status of key risk indicators. It is possible to have multiple action plans associated with a given issue. You can also link an action plan to multiple issues or other types of business objects.

The following is a simple workflow used by Orion Star to develop an issue and action plan when a fraud loss exceeds \$10,000.

Display 3.9 Issues and Action Plans Workflow at Orion Star for Fraud Losses


For more information about implementing issues and action plans through the SAS Enterprise GRC user interface, see [Chapter 8, “Implementing Issues and Action Plans,”](#) on page 87.

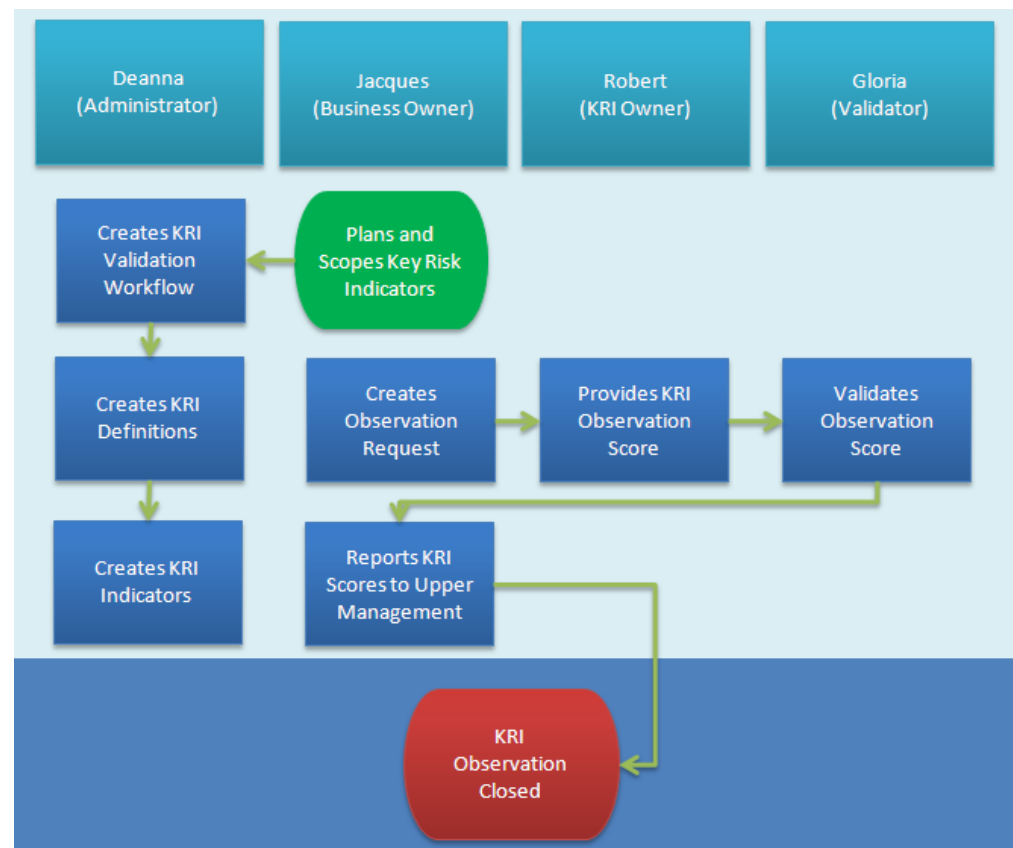
Defining Key Risk Indicators

Key risk indicators, or KRIs, are a way for management to measure the risk and control profile of an organization as it operates over time, by defining and setting thresholds on

risks that could indicate a problem in the organization. For example, if an organization suffers from increasing system downtime, measured by number of outages or total downtime, it could be an indicator of future losses as customers look for alternatives to the business. Managers within the organization should decide which key risk indicators are most important to track within the organization, based on internal or consortium data. Setting an appropriate threshold on KRIs is just as important as determining which risks should be monitored. Threshold levels might need to be monitored and modified over time, depending on the indicator.

The following is a workflow used by Orion Star to regularly validate a KRI that follows the number of failed trades on a monthly basis within the Securities department.

Display 3.10 Key Risk Indicators Workflow at Orion Star for Securities Department



For more information about implementing KRIs through the SAS Enterprise GRC user interface, see [Chapter 9, “Implementing Key Risk Indicators \(KRIs\) and KRI Workflows,”](#) on page 97.

Developing Controls and Control Tests

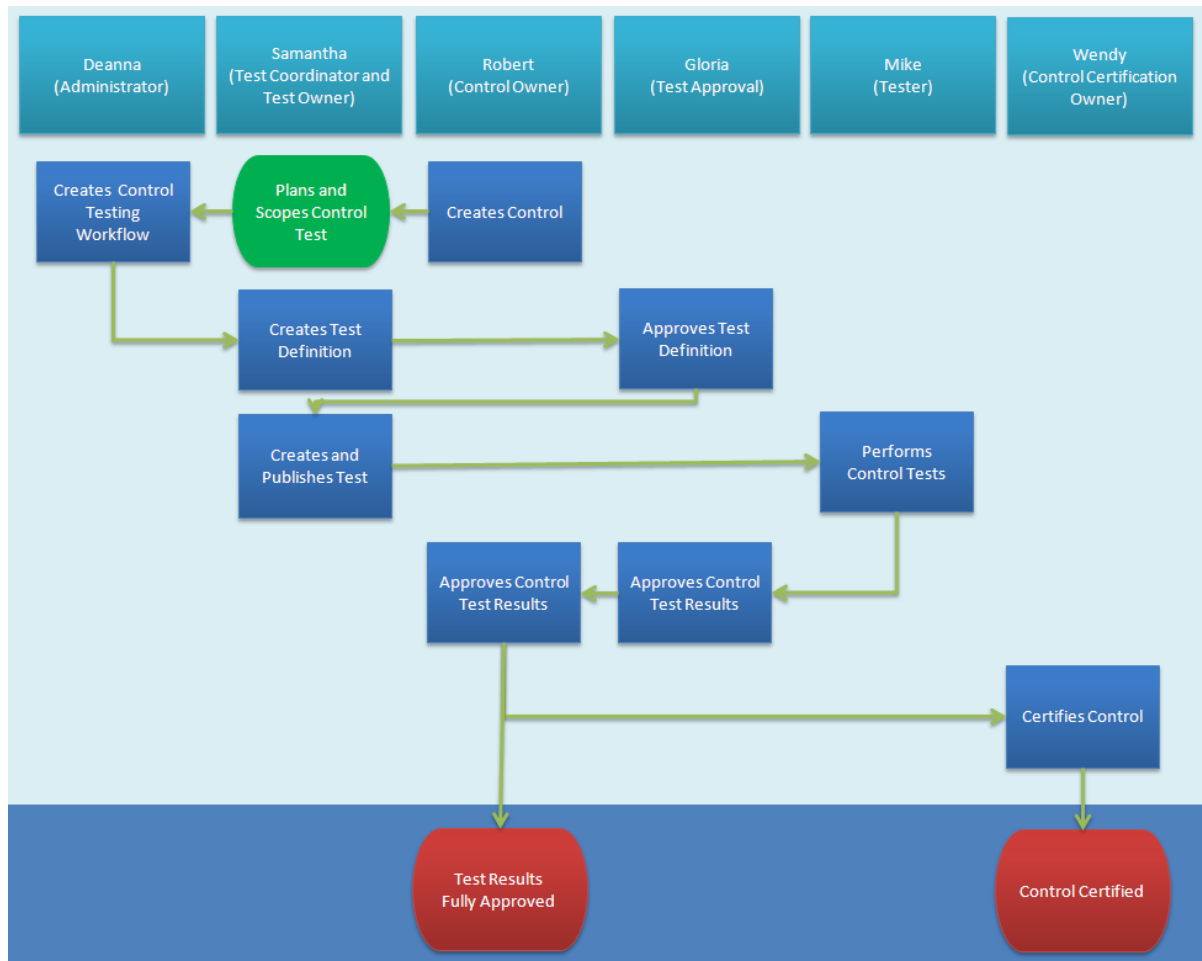
Controls are methods to reduce risk within an organization. An example of a control would be segregation of duties, which requires more than one person to complete a business transaction, in order to reduce the risk of internal fraud by one individual.

It is important to have a full understanding of the risks that your organization faces when developing controls. Controls cannot mitigate all risk, but they can often greatly reduce the risk to a sustainable level.

In order for controls to be effective, controls should be regularly tested for adequacy and effectiveness. This is done through a control test and certification process.

Orion Star has implemented controls to mitigate some of the risks that they have identified. And they have developed a control certification process to regularly test these controls and ensure that they are effective. One of the risks that Orion Star has identified during the risk assessment process is that a network intrusion could disrupt business or leak sensitive data, which exposes them to financial risk. In order to mitigate this risk, the IT department at Orion Star has installed a redundant network firewall system. This hardware control keeps attackers from compromising the network. This control must be tested regularly to ensure that in the event that a device fails, business can be conducted as usual. Orion Star has set up a monthly process for the IT Security Analyst to test the effectiveness of the firewall for the Securities department. The IT Security Analyst then certifies that the firewall is working properly to mitigate the risk of network intrusion. The following is a process example to develop and test the firewall.

Display 3.11 Control Testing Workflow at Orion Star for Network Firewall Device



For more information about implementing controls and control tests through the SAS Enterprise GRC user interface, see [Chapter 10, “Implementing Controls and Control Tests,”](#) on page 111.

Managing Incidents

Organizations use incident management to track events that occur within the organization over time and to account for outcomes related to these events, such as losses, recoveries, and other financial or nonfinancial impacts.

Orion Star is using SAS Enterprise GRC to capture and investigate incidents and link them to financial effects, nonfinancial effects, risks, controls, and so on. As these incidents occur, Orion Star can use the data and object links to assess the effectiveness of their controls, create issues and develop action plans, and so on.

For more information about managing and investigating an example incident, see [“Managing Incidents and Incident Workflows” on page 169](#).

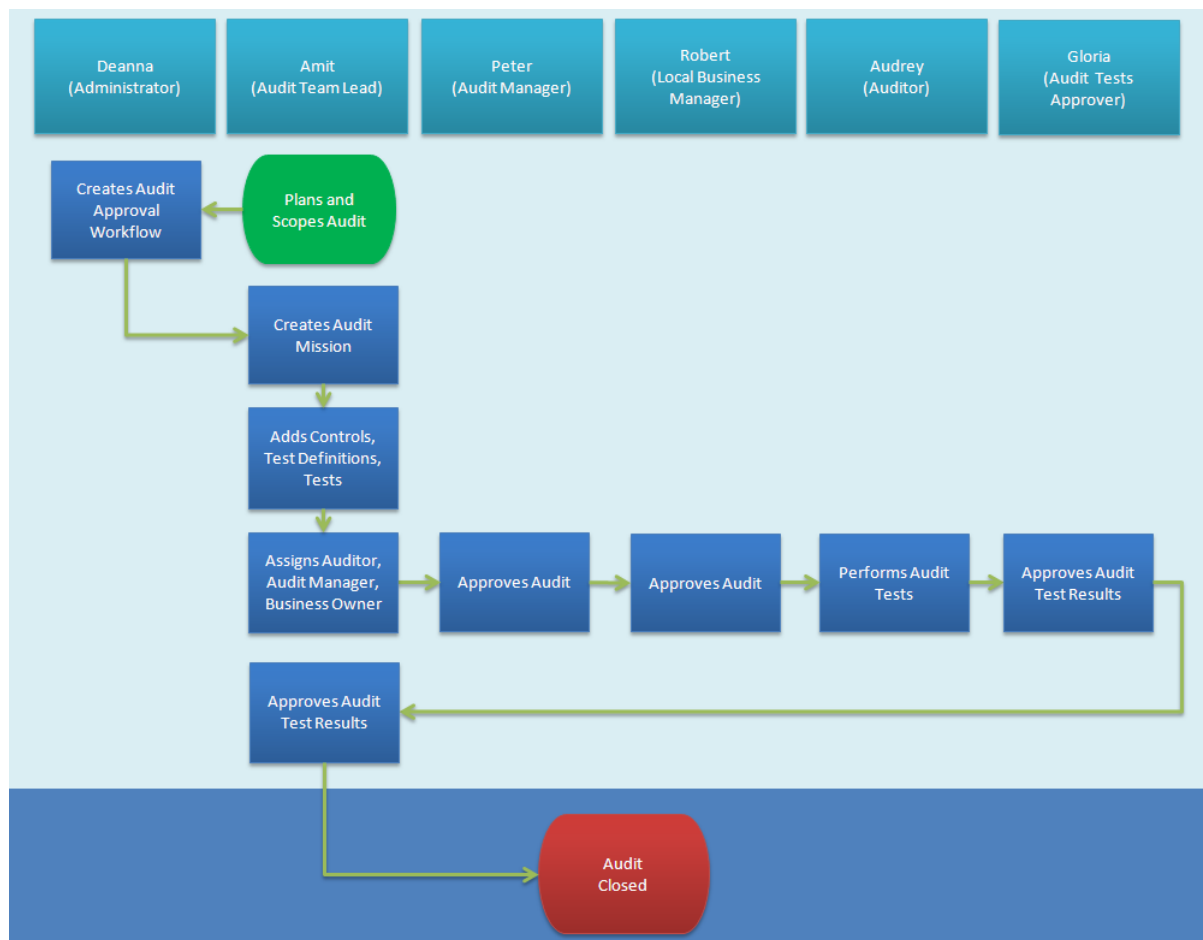
Developing Audits

Audits are intended to provide an objective evaluation of an organization's controls. Audit missions are similar to control tests, in that auditors assess one or more controls on a periodic basis and determine the adequacy and effectiveness of controls. However, audits differ in that you can plan for audits and conceal specific information about the audit from the group being audited. The default audit mission enables the group being audited to approve the audit mission without knowing the specific details, such as the exact date of the audit. Unlike control tests, there is no control certification process in place for audits.

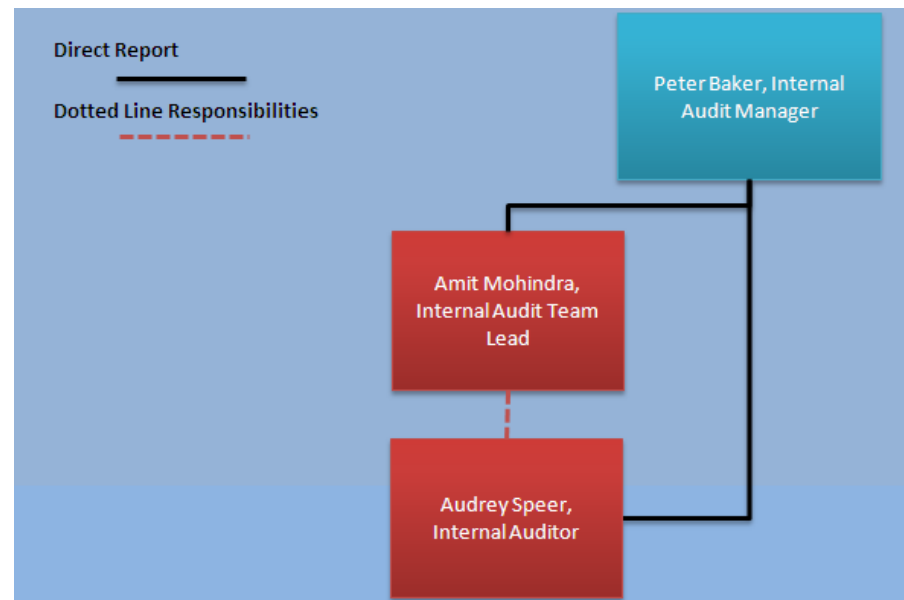
Orion Star has implemented an audit mission to determine whether the network firewall device properly fails over. Although the control is regularly tested and certified by the IT group at Orion Star, internal auditors are brought in to perform objective tests and ensure that the device is working as certified. An audit is conducted at a random time to test the network firewall. The auditor tests the firewall and then enters the audit results, which are approved by the audit tests approver.

The following is a process example for the network firewall audit.

Display 3.12 Audit Mission Workflow at Orion Star for Network Firewall Device



For the purposes of understanding the additional roles needed to carry out these activities, the following organizational chart displays some of the internal auditors and their role or roles in auditing Orion Star.

Display 3.13 Internal Audit Organizational Chart

The following table describes a subset of audit-specific users and their defined roles and responsibilities in auditing Orion Star.

Table 3.2 Users, Roles, and Responsibilities at Orion Star

User	Job Title	Responsibility	Enterprise GRC Roles Used for This Example
Peter Baker	Audit Manager	Manages the internal audit team.	Enterprise GRC: Audit Management
Amit Mohindra	Audit Team Lead	Responsible for creating audit missions and leading the internal audit team.	Enterprise GRC: Audit Team Leadership
Audrey Speer	Auditor	Performs the audit.	Enterprise GRC: Auditing

For more information about implementing audit missions through the SAS Enterprise GRC user interface, see [“Implementing Audit Missions” on page 123](#).

Chapter 4

Implementing the Business Structure

Overview	49
Using the Dimension Browser	50
Overview	50
Example: Creating a Node	52
Example: Moving a Node	53
Splitting Nodes	54
Merging Nodes	56
Mappings	59
Overview	59
Example: Adding Item Process Mappings	60
Processes	61
Overview of Processes	61
Example: Creating a Process Instance	62
Objectives	62
Overview of Objectives	62
Example: Creating an Objective Instance	62
Obligations	63
Overview of Obligations	63
Example: Creating an Obligation	63

Overview

Before you can manage and monitor GRC activities in SAS Enterprise GRC, your organization must build an environment suitable for risk analysis. One of the first steps is to implement the business structure. This requires collecting organizational data and creating a number of hierarchical constructs called *dimensions*, as well as creating specific instances of some dimensions, such as processes and objectives. This chapter is intended to provide information about using the default user interface and sample data to modify the business structure in SAS Enterprise GRC. For more information about the example used here and the process of gathering organizational data, see [Chapter 3, “Gathering Governance, Risk, and Compliance Data,”](#) on page 27.

After information has been gathered about business structure dimensions, a SAS Enterprise GRC system administrator typically implements the majority of these dimensions through the user interface. These dimensions can be constructed in the user interface or command-line through the data loader process, or manually in the **Administration** menu under the **Business Structure** submenu.

The **Administration > Business Structure** submenu enables you to perform the following tasks:

- Manage dimensions. You must have the View Dimension Browser capability to view the Dimension Browser window.
- Manage mappings. You must have the View Mappings capability to view the Mappings window.
- Manage processes. You must have Process Instance capabilities to view the Processes window.
- Manage objectives. You must have Objective Instance capabilities to view the Objectives window.
- Manage obligations. You must have Obligation capabilities to view the Obligations window.

This chapter uses the default environment for the example provided in [Chapter 3, “Gathering Governance, Risk, and Compliance Data,”](#) on page 27. The example environment uses the sample data that is provided with the product. The SAS Enterprise GRC environment is highly customizable, so your organization's tasks might vary depending on the level of customization involved.

For more detailed information about other administrative tasks, such as product installation, customization, configuration, assigning roles and capabilities to users, and data management, see the *SAS Enterprise GRC: Administration and Customization Guide*.

Using the Dimension Browser

Overview

In SAS Enterprise GRC, the structure of your GRC organization is defined within a multidimensional space, which can be subset into the following five spaces:

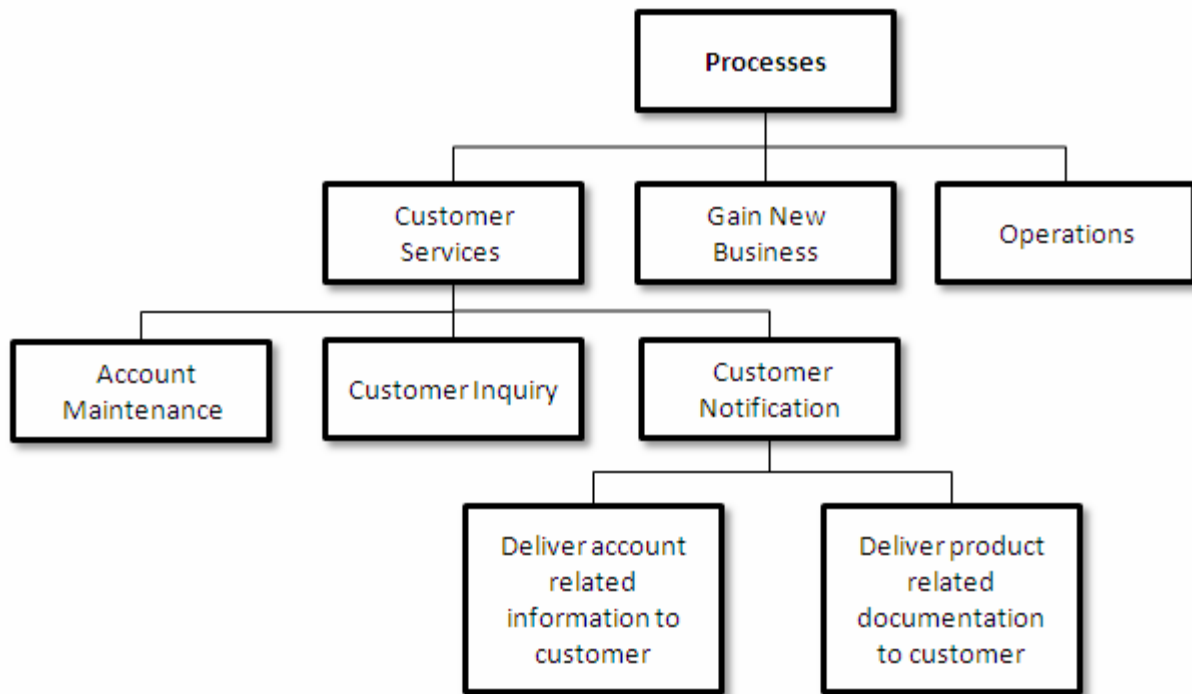
- Organizational
- Operational
- Risk Classification
- Risk Management
- Reporting

Each dimension is an element of exactly one of these spaces. Examples of dimensions in the Organizational space include Management Organization, Business Line, Cost Center, Geography, and Legal Organization. For more information about the types of spaces and dimensions, see "Overview of Dimensionality" in the *SAS Enterprise GRC: Administration and Customization Guide*.

Each dimension consists of a hierarchy of dimensional elements, each of which are called *nodes*. For example, the Process Type dimension, a type of operational dimension, might include three nodes: Customer Services, Gain New Business, and Operations. The subset of Customer Services that are related to the Customer Notification node might include the nodes **Deliver account related information to customers** and **Deliver product related documentation to customers**.

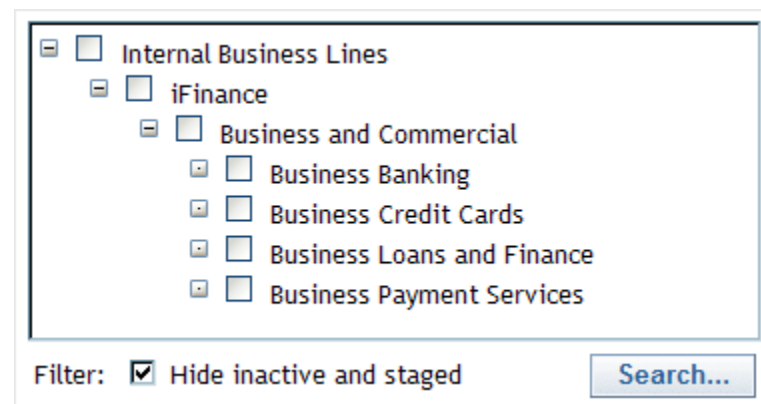
The following figure displays a partial representation of how the Process Type dimension might be structured. Not all nodes are displayed.

Display 4.1 Example of a Dimensional Structure: Process Dimension



SAS Enterprise GRC displays dimensions in a navigation tree. The following figure displays a navigation tree for the Business Line dimension.

Display 4.2 Example Navigation Tree



By working with a number of dimensions in this way, you can assign GRC activities to these dimensions and improve your interaction with GRC data. For example, if an incident occurs in which business credit card accounts have been compromised, and if the company fails to properly notify customers, this can result both in financial loss and reputational loss. This risk can be seen both as a failure in the Business Credit Cards business line and as a failure in its Customer Notification process. Organizations can use dimensions in multiple ways to classify risks, controls, and other factors, and ultimately can make decisions to reduce and accept organizational risks.

Each dimension can contain the following types of nodes:

Node

A node is an element of the tree. In the example navigation tree, Internal Business Lines, iFinance, Business and Commercial, Business Banking, Business Credit Cards, Business Loans and Finance, and Business Payment Services are all nodes.

Ancestor

An ancestor node precedes another node. In the example navigation tree, iFinance is an ancestor of Business Credit Cards. Internal Business Lines is the only node that does not have an ancestor.

Parent

A parent node immediately precedes another node. In the example navigation tree, Internal Business Lines is the parent of iFinance, and iFinance is the parent of Business and Commercial. Internal Business Lines is the only node that does not have a parent. A parent node is a special case of an ancestor node.

Descendant

A descendant node follows another node. In the example navigation tree, Business Credit Cards is a descendant of iFinance.

Child

A child node immediately follows another node. In the example navigation tree, iFinance is a child of Internal Business Lines. Business Banking and Business Credit Cards are both children of Business and Commercial. A child node is a special case of a descendant node.

Root

A root node has no parent. In the example navigation tree, Internal Business Lines is the root node. Every dimension has exactly one root node.

Leaf

A leaf node has no children. In the example navigation tree, Business Banking, Business Credit Cards, Business Loans and Finance, and Business Payment Services are all leaf nodes.

A subtree can be created from a tree at any node of the original tree. The node used to define the subtree becomes the root node of the subtree. All descendant nodes of that node are also included in the subtree.

Example: Creating a Node

Suppose that Orion Star has operations in Chile, and you want to create a new node named Chile and use Geographies > Americas > South America as its parent. To create this new node:

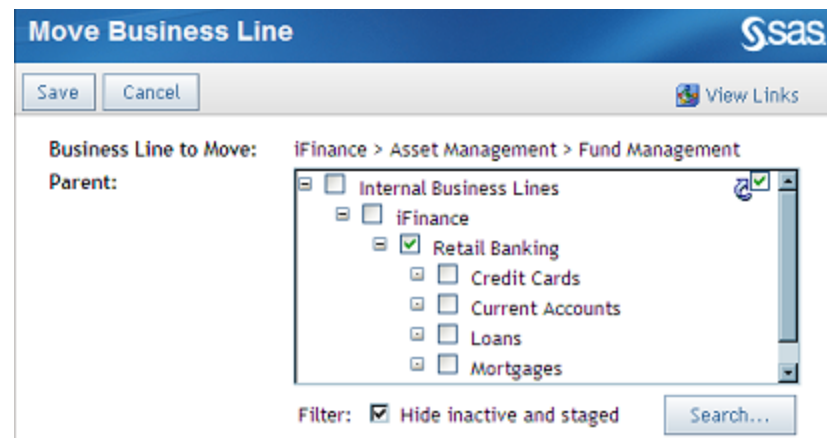
1. Select **Administration > Business Structure > Dimension Browser** from the menu.
2. From the **Dimension** drop-down list, select the **Geography** dimension.
3. Click **Create Geography**.
4. Select **Geographies > Americas > South America** as the **Path** to the new node.
5. Enter Chile as the **Geography Name**.
6. Accept the defaults for the remaining fields.
7. Click **Save**. The View Geography window appears with the new node.
8. Click **Done** to exit the View Geography window.

Display 4.3 Example Create Geography Window

Example: Moving a Node

Suppose that Orion Star is moving the Fund Management business line, which is currently under Asset Management, under the Retail Banking umbrella. To capture this change in SAS Enterprise GRC, you want to move the Fund Management node from Internal Business Lines > iFinance > Asset Management to Internal Business Lines > iFinance > Retail Banking. To move this node:

1. Select **Administration > Business Structure > Dimension Browser** from the menu.
2. From the **Dimension** drop-down list, select the **Business Line** dimension.
3. Select the **iFinance > Asset Management > Fund Management** node. The **View Business Line** window appears.
4. Click **Move**. The **Move Business Line** window appears.
5. Select **Internal Business Lines > iFinance > Retail Banking** as the **Parent**.
6. Click **Save**. The **Change Reason** window appears.
7. Enter the reason for the change and then click **Save**.
8. Click **Done** to exit the **View Business Line** window.

Display 4.4 Example Move Business Line Window

Splitting Nodes

Overview

The Split wizard enables you to create or edit a batch file that an administrator can run to split a node into two nodes. The additional node that is created does not have to have the same parent as the original node. In the Split page of the Split wizard, you can choose whether to edit an existing split file or to create a new split file. In addition, after you have entered the properties of the new node, you can generate a draft of the split file. This feature enables you to interrupt your work on a split file and to return to it later. You save your draft and load it when you are ready to work on it again. The behavior of the Split wizard is the same regardless of whether you are creating a new split file or editing an existing split file.

In the wizard, you must make decisions about what to do with objects such as positions and losses that are associated with the node that you are splitting. The Split wizard is supported for the following objects:

- ActionPlan
- Assessment
- AssessmentTrigger
- CauseInstance
- ControlInstance
- DimChildren
- DimRelMapping
- Event
- Incident
- Issue
- Loss
- Position
- QuestionGroup
- Recovery

- RiskInstance
- SupportiveQuestionnaire

For each object, you can choose one of the following actions:

- Move. This action moves the object into the new node. It is no longer in the original node.
- Keep. This action keeps the object in the original node. It is not in the new node.
- Copy. This action copies the object into the new node. It is also in the original node.

When you run a split file, each object is kept, moved, or copied according to the directions in the file. This process does not work when the object is being edited by another user and is in validation. Therefore, the execution of splits must occur in batch when the system is offline.

For more information about how to use command-line tools to run a split file, see "Data Administration" in the *SAS Enterprise GRC: Administration and Customization Guide*.

Your ability to split a dimension depends on the `split.enable` properties of the dimension, which can be customized by an administrator. For more information, see "Customizing SAS Enterprise GRC" in the *SAS Enterprise GRC: Administration and Customization Guide*.

Example: Creating a Split File

Orion Star is changing its legal organization, and the Group Holdings team is creating a new legal team called Commercial Group Holdings. In SAS Enterprise GRC, you want to split the Legal Organizations > iFinance Group Holdings node. This split process creates a new node named iFinance Commercial Group Holdings, which is a child node of Legal Organizations.

There are two basic steps to the process. First, you must use the Web application to create a split file. Second, an administrator must use the SAS Enterprise GRC administrative tools to submit the split file. This second step performs the actual split.

Note: This example assumes that there is a mapping, a position, and an issue in the iFinance Group Holdings node.

To create a split file in the Web application:

1. Select **Administration > Business Structure > Dimension Browser** from the menu.
2. From the **Dimension** drop-down list, select the **Legal Organization** dimension.
3. Select the **iFinance Group Holdings** node. The **View Legal Organization** window appears.
4. Click **Split**. The Split wizard opens.
5. Select the **Tasks to perform**. To follow this example, you should select mappings, positions, and issues. Click **Next**.
6. Enter the details of the split:
 - a. Enter iFinance Commercial Group Holdings as the **Organization Name**.
 - b. Select Legal Organizations as the **Parent**.
 - c. Enter the **Justification** for the split.
 - d. Accept the defaults for the remaining fields. Click **Next**.

7. Select the children that you want to move in the split. The iFinance Group Holdings node has five child nodes.

Display 4.5 Example Children Page of Split Wizard

Select the children to move:

<input type="checkbox"/>	Name
<input type="checkbox"/>	iFinance Asset Management Group
<input type="checkbox"/>	iFinance Business and Commercial Banking Group
<input type="checkbox"/>	iFinance Insurance Group
<input type="checkbox"/>	iFinance Investment Banking Group
<input type="checkbox"/>	iFinance Retail Banking Group

In this example, select only the **iFinance Business and Commercial Banking Group** and **iFinance Investment Banking Group** nodes as child nodes to move. The other three child nodes remain in the original node. Click **Next**.

8. Select to Keep the mapping. Click **Next**.
9. Select to Copy the position. Click **Next**.
10. Select to Move the issue. Click **Next**.
11. Click **Generate Split File**.
12. Click **Save**. The downloaded split file should be given to an administrator so that the split file can be submitted.
13. Click **Cancel** to return to the View Legal Organization window.
14. Click **Done** to exit the View Legal Organization window.

Merging Nodes

Overview

The **Merge Dimension** window enables you to create a batch file that an administrator can run to merge a dimensional element with another dimensional element.

A merge causes the dimensional element that is merged to become invisible in the product. Related objects appear under the new node. Both the dimensional element and its related records remain in the database for auditing purposes.

When a merge file is run, each object is moved or copied according to the directions in the file, regardless of whether an object is in validation. If two dimensional elements are merged and only one of the elements has validation stages assigned to it, then the assigned stages persist in the dimensional element that results from the merge. However, if a dimensional element with validation stages is merged into another dimensional element with validation stages, then only the stages that are assigned to the dimensional element into which the other element was merged remain.

Note: The execution of merges has to occur in batch when the system is offline.

For more information about how to use command-line tools to run a merge file, see "Data Administration" in the *SAS Enterprise GRC: Administration and Customization Guide*.

Your ability to merge dimensions depends on the **merge.enable** properties of the merging dimensions, which can be customized by an administrator. For more information, see "Customizing SAS Enterprise GRC" in the *SAS Enterprise GRC: Administration and Customization Guide*.

Example: Creating a Merge File

Orion Star is merging the Retail Banking division into Asset Management. In SAS Enterprise GRC, you want to merge the Internal Business Lines > iFinance > Retail Banking and Internal Business Lines > iFinance > Asset Management nodes. This example merge process merges the Retail Banking node into the Asset Management node.

There are two basic steps to the process. First, you must use the Web application to create a merge file. Second, an administrator must use the SAS Enterprise GRC administrative tools to submit the merge file. This second step performs the actual merge.

To create a merge file in the Web application:

1. Select **Administration > Business Structure > Dimension Browser** from the menu.
2. From the **Dimension** drop-down list, select the **Business Line** dimension.
3. Select the **iFinance > Retail Banking** node. The **View Business Line** window appears.
4. Click **Merge**. The **Merge Business Line** window appears.

Display 4.6 Example Merge Business Line Window

Merge Business Line sas

View Merge Analysis Report Cancel

Path: iFinance -> Retail Banking

Children: Credit Cards
Current Accounts
Loans
Mortgages
Savings
Fund Management

* Destination:

- ☐ Internal Business Lines
 - ☐ iFinance
 - ☒ Asset Management

Filter: ☒ Hide inactive and staged Search...

All children, objects, and mappings will be moved.

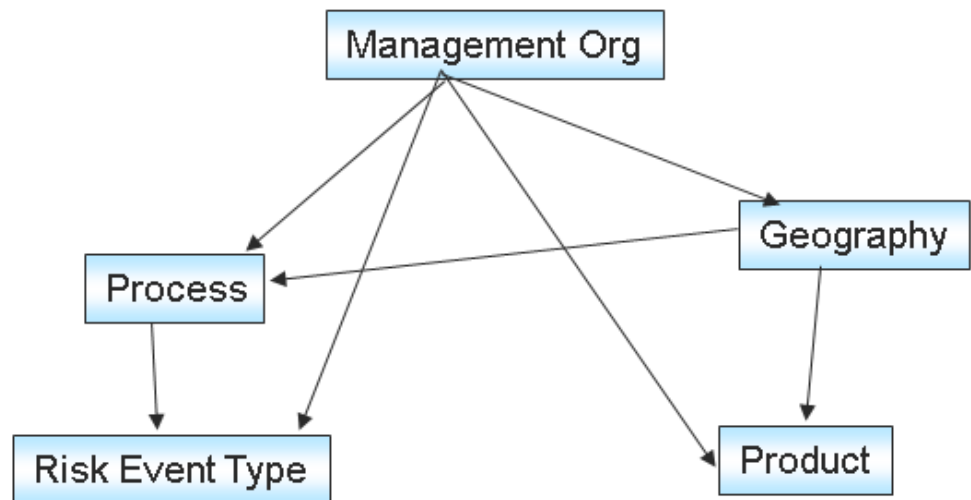
* Justification

5. Select **Internal Business Lines > iFinance > Asset Management** as the Destination.
6. Enter the **Justification** for the merge.
7. Click **View Merge Analysis Report**.
8. View the report and click **Download Merge File**.
9. Click **Save**. The downloaded merge file should be given to an administrator so that the merge file can be submitted.
10. Click **Cancel** to return to the **View Business Line** window.
11. Click **Done** to exit the **View Business Line** window.

Mappings

Overview

Mappings are constructs in SAS Enterprise GRC that enable you to control or enforce dimensional relationships. For example, if you are selecting an operational point for a management organization and want to display only processes relevant to that particular organization for selection, you can create that filter using a mapping. The following figure shows how any dimension can be mapped to any other dimension.



In SAS Enterprise GRC, mappings are constructed from an operational point and a *mapping type*. Mapping types are dimensional relationships between a domain and a co-domain. These relationships are either hardcoded in the system or defined in the dimensionality.xml file. For information about the default and hardcoded mapping types, see "Customize Dimensionality" in the *SAS Enterprise GRC: Administration and Customization Guide*.

Note: You cannot create or edit mapping types in the Web application.

Each mapping type is mapped in a 1:1 or n:1 relationship between its domain and co-domain. The co-domain always has exactly one dimension. A 1:1 mapping relates a one-dimensional domain to a corresponding one-dimensional co-domain. An n:1 mapping relates a multi-dimensional domain mapped to the one-dimensional co-domain. For example, the domain of the Process Execution Map has the following dimensions: Management Organization, Business Line, Legal Organization, Geography, and Cost Center.

When you select a mapping type in the **Mappings** window, the selections that are available to you depend on the operational point that you selected. You can select only the mapping types whose domain contains any of the dimensions of the selected operational point. For example, if you select Financial Statement Item > Balance Sheet, then you can select either Item Assertion Map or Item Process Map. These are the only two mapping types whose domain contains the Financial Statement Item dimension.

After you have chosen the operational point and the mapping type, you can add a mapping. You add a mapping by selecting a node of a dimension. The dimension from which you select a node is the dimension of the co-domain of the mapping type that you chose.

Example: Adding Item Process Mappings

For Orion Star, risk management processes are a vital part of maintaining a healthy balance sheet, whereas GRC processes specifically affect assets on its balance sheet. In SAS Enterprise GRC, Orion Star wants to create a relationship between these dimensional elements by mapping nodes of the Financial Statement Item dimension to nodes of the Process dimension. The first step is to find a mapping type to support the mappings. Fortunately, in dimensionality.xml, there is a dimensional relation named Item Process Map, which supports the mappings that you want to add.

To add these two Item Process mappings:

1. Select **Administration > Business Structure > Mappings** from the menu.
2. Select **Financial Statement Item > Balance Sheet** as the operational point.
3. Select **Item Process Map** as the **Mapping Type**.
4. Click **Add Mapping** in the Mappings table. The Add Mapping window appears.
5. Select **Risk Management** in the Process dimension tree.
6. Click **OK**. You are returned to the Mappings window.
7. Select **Financial Statement Item > Balance Sheet > Assets** as the operational point.
8. Select Item Process Map as the **Mapping Type**.
9. Check the **Show Inherited** box. The first mapping that you added is displayed in the Mappings table.
10. Click **Add Mapping** in the Mappings table. The **Add Mapping** window appears.
11. Select **Operations** in the Process dimension tree.
12. Click **OK**. You are returned to the **Mappings** window.

The first mapping that was added mapped **Financial Statement Item > Balance Sheet** to **Process > Risk Management**. The second mapping that was added mapped **Financial Statement Item > Balance Sheet > Assets** to **Process > Operations**. These two mappings are displayed in the Mappings table.

Display 4.7 Example Item Process Mappings

Mappings

Operational Point

Edit | Clear | Favorites▼

Financial Statement Item: Balance Sheet > Assets




Mapping Type


Item Process Map

☒ Show Inherited

Mappings (2)

Add Mapping... | Remove Selected Mappings

	Relative Weight	ID	Dimensional Point	Name	Owner
		12409	Financial Statement Item: Balance Sheet	Process: Risk Management	
<input type="checkbox"/>		12405	Financial Statement Item: Balance Sheet > Assets	Process: Operations	

The operational point that is selected is Financial Statement Item > Balance Sheet > Assets. The Inherited Mapping icon  next to the first mapping indicates that the mapping is inherited from the Financial Statement Item > Balance Sheet node.

Inherited mappings cannot be deleted directly. To delete this mapping, you first have to change the operational point to Financial Statement Item > Balance Sheet.

Processes

Overview of Processes

Processes are used for implementing and managing organizational policies. Policy administrators and other GRC officers can link processes to policies and use this association to track the effectiveness of processes in following policy statements. Each process instance is associated with one process dimension. To view the example process dimension tree, see [Display 4.1 on page 51](#).


For example, Orion Star has a process dimension node as follows: Processes > Customer Services > Customer Notification > Deliver account related information to customers. Under this dimension, there is a business process called Deliver monthly balance for asset management customers in the iFinance > Investment Banking > Securities organization to send monthly statements to customers and notify them of their balance. In order to account for this business process, a process instance must be created in the system.

The process instance is eventually tied to a policy that requires that all customers receive a monthly notification of their balance. When the policy that tracks this process is later

created, you can link the process to the policy. For more information about creating policies, see [“Managing Organizational Policies” on page 77](#).

Example: Creating a Process Instance

To create this process instance:

1. Select **Administration > Business Structure > Processes** from the menu.
2. Click **Create Process**. The Create Process window appears.
3. Select the Management Organization **iFinance > Investment Banking > Securities** as the operational area.
4. Select **Processes > Customer Services > Customer Notification > Deliver account related information to customers** in the **Process Type** tree.
5. Enter *Deliver monthly balance for asset management customers* in the **Process Title** field.
6. (Optional) Enter a **Process Description**.
7. The Securities department policy administrator, Aniela Olesky, owns this process. Click the Select User icon () in the **Process Owner** field. Select **Aniela Olesky** as the process owner.
8. Click **Save** to save the process and return to the previous window.

Objectives

Overview of Objectives

Objectives refer to certain achievable business or governance objectives. Policy administrators and other GRC officers link objectives to policies in order to determine whether the policy is effective in helping the organization achieve its objectives. Like processes, each objective instance is associated with one objective dimension.


For example, Orion Star has an objective dimension node as follows: **Objectives > Investment Banking > Reduce costs by 4.5%**. Under this dimension, there is an objective called **Reduce Web and external E-mail use** that is to be created in the **iFinance > Investment Banking** organization.

The objective instance can eventually be tied to an example policy that discourages employees from using external e-mail systems. For more information about the example policy, see [“Implementing an Example Policy” on page 81](#).

Example: Creating an Objective Instance

To create this objective instance:

1. Select **Administration > Business Structure > Objectives** from the menu.
2. Click **Create Objective**. The Create Objective window appears.
3. Select the Management Organization **iFinance > Investment Banking** as the operational area.

4. Select **Objectives > Investment Banking > Reduce costs by 4.5%** in the **Objective** tree.
5. Enter *Reduce Web and external e-mail use* in the **Objective Title** field.
6. Enter an **Objective Description**, such as *To reduce the cost of IT infrastructure.*
7. The Securities department policy administrator, Aniela Olesky, owns this objective. Click the Select User icon () in the **Owner** field. Select **Aniela Olesky** as the objective owner.
8. Click **Save** to save the objective and return to the previous window.

Obligations

Overview of Obligations

Obligations are requirements that must be met in order for an organization to comply with laws or regulations. Policy administrators and other GRC officers link objectives to policies in order to ensure that the policy meets these requirements.


For example, Orion Star has a corporate obligation to comply with the United States Securities and Exchange Commission (SEC) regulations. In order for the organization to meet this obligation, a policy exists to train all employees annually on SEC regulations. This policy is designed to ensure that all iFinance employees are aware of SEC regulations and comply with them.

The obligation can eventually be tied to an SEC regulation policy. For more information about creating policies, see [“Managing Organizational Policies” on page 77](#).

Example: Creating an Obligation

To create this obligation instance:

1. Select **Administration > Business Structure > Obligations** from the menu.
2. Click **Create Obligation**. The Create Obligation window appears.
3. Select the Management Organization **iFinance** as the operational area.
4. Select **Government** as the **Obligation Type**.
5. Enter *Comply with the Securities and Exchange Act of 1934* in the **Obligation Title** field.
6. (Optional) Enter an **Obligation Description**.
7. Enter *SEC* as the **Agency Name**.
8. Select **National** as the **Agency Type**.
9. Enter *48 Stat 881* as the **Reference Number**.
10. Enter *The Securities and Exchange Act of 1934* as the **Official Location Name**.
11. Select the date on which the regulation was enacted in the **Enacted Date** field (for example, 6/6/1934).
12. Select the **Effective From Date** and **Effective To Date**.

13. The chief risk officer, Gustav Mueller, owns this obligation. Click the Select User icon () in the **Obligation Owner** field. Select **Gustav Mueller** as the obligation owner.
14. Click **Save** to save the obligation and return to the previous window.

Chapter 5

Implementing Users, Roles, and Responsibilities

Overview	65
Implementing Users	66
Implementing Roles	66
Example: Assigning a Role and Scope to a User	67

Overview

Each user of the system is assigned one or more roles to carry out their organizational responsibilities in SAS Enterprise GRC. The system provides a flexible and customizable environment that enables an administrator to adapt to the size, structure, and nature of the organization. This chapter is intended to provide information about using the default user interface and sample data to load users, roles, and responsibilities into SAS Enterprise GRC, and to assign each user to a scope and role.

After information has been gathered about users, roles, and responsibilities, a SAS Enterprise GRC system administrator typically implements users, roles, and responsibilities through the SAS Management Console. For more information about the process of gathering organizational data, see [Chapter 3, “Gathering Governance, Risk, and Compliance Data,”](#) on page 27.

This chapter uses the default environment for the example provided in [Chapter 3, “Gathering Governance, Risk, and Compliance Data,”](#) on page 27. The example environment is based on the sample data that is provided with the product. Your organization's tasks might vary depending on the level of customization involved.

This chapter focuses specifically on implementing users and roles in SAS Enterprise GRC. See [“Performing Other Administrative Tasks”](#) on page 195 for information about other administrative tasks that you can perform in the SAS Enterprise GRC **Administration** menu.

For more detailed information about other administrative tasks that are not available through the user interface, such as product installation, customization, configuration, assigning roles and capabilities to users, and data management, see the *SAS Enterprise GRC: Administration and Customization Guide*.

Implementing Users

Before a user can log on to SAS Enterprise GRC, the user must exist in the User table and also in the SAS Metadata server. The SAS Metadata server supports fields for users such as name, title, e-mail addresses, and phone numbers. However, it does not support fields such as security clearance, default locations, assigned positions, and assigned validation stages. Therefore, it is necessary to have user data in both SAS Enterprise GRC and SAS Metadata.

In SAS Metadata, all SAS Enterprise GRC users must be placed either in the **Enterprise GRC Users** group, which contains all application users, or the **Enterprise GRC Data Administrators** group, which contains all administrative users. You should not place a user in both groups.

The Users window enables you to synchronize SAS Enterprise GRC users with SAS Metadata users. When you synchronize users, the two separate sources of users are compared using the User Name from SAS Metadata and the User ID from SAS Enterprise GRC. The comparison results in one of the three following actions:

- Users that are in SAS Metadata but not SAS Enterprise GRC are created in the application. Fields that are defined in SAS Metadata are not editable in the application. All application-specific fields such as position, security clearance, and default location are set to **missing**. Before a user can perform any task in SAS Enterprise GRC, that user must be assigned to at least one position.
- Users that are in SAS Enterprise GRC but not SAS Metadata are set to **inactive**.
- Users that are in both sources have fields that are defined in SAS Metadata updated in the application.

For information about defining users in SAS Metadata, see the *SAS Intelligence Platform: Security Administration Guide*.

For information about defining users in SAS Enterprise GRC, see the “Overview of Synchronizing Users, Roles, and Capabilities and Loading User Positions” in the *SAS Enterprise GRC: Administration and Customization Guide*.

SAS Metadata enables you to specify multiple e-mail addresses and phone numbers. These multiple values are stored in SAS Enterprise GRC as comma-delimited values.

Implementing Roles

When you log on to SAS Enterprise GRC, the application examines your positions in the Users table. Each position is defined by a scope and a role. Each role has capabilities associated with it. Therefore, the role determines what you can do in the application. The scope determines where you can do things in the application.

Roles must first be loaded in SAS Metadata and are then made available in the application by an administrator through a role synchronization process.

The Roles window enables you to view the capabilities of each role and to synchronize SAS Enterprise GRC roles with SAS Metadata roles. When you synchronize roles, the two separate sources of roles are compared using the Role Name from SAS Metadata and the Role ID from SAS Enterprise GRC. Like the user synchronization process, the comparison results in one of the three following actions:

- Roles that are in SAS Metadata but not SAS Enterprise GRC are created in the application.
- Roles that are in SAS Enterprise GRC but not SAS Metadata are set to **inactive**.
- Roles that are in both sources have fields that are defined in SAS Metadata updated in the application.

In addition, there is a hardcoded user named *grcadmin*. The role of the *grcadmin* user is the Enterprise GRC: Administration role. The scope of the *grcadmin* user is Everywhere. This position means that the *grcadmin* user can do anything in the application, regardless of the location of the object.

For more information about security management, role assignment, and descriptions of the capabilities, see “Security and Role Administration” in the *SAS Enterprise GRC: Administration and Customization Guide*.

Example: Assigning a Role and Scope to a User

Before assigning a role and scope to a user, a user must first be assigned a role in SAS Metadata. This is done through the SAS Management Console. For more information about using the SAS Management Console, see “Security and Role Administration” in the *SAS Enterprise GRC: Administration and Customization Guide*.

After you have implemented roles and users and assigned users to the appropriate roles in SAS Metadata, you can assign a role and scope to a user in SAS Enterprise GRC. An example Select a Role and Scope window is displayed in the following figure. Suppose that you want to assign Jacques Simon, the Central Operational Risk Manager for the Investment Banking division, a role of Business Owner and a scope of Business Line > iFinance > Investment Banking. You can add this position using the following steps in the default environment:

1. Select **Administration > Users** from the menu.
2. Click on an attribute of Jacques in the Users table. The Edit User window appears.
3. In the Assigned Positions table, click **Add**. The Select a Role and Scope window appears.
4. Under the **Select a Role** drop-down list, select **Enterprise GRC: Business Ownership**.
5. In the OL Chooser, click **New Point**. The New Operational Point window appears.
6. Under the **Dimension** drop-down list, select **Business Line**. Browse through the tree and select the business line scope **Internal Business Lines > iFinance > Investment Banking**. Click **Add and Close**. You are returned to the Select a Role and Scope Window.
7. Select the role **Enterprise GRC: Business Ownership**, and click **Add**. You are returned to the Edit User window.

Display 5.1 Example Select a Role and Scope Window

SAS Enterprise GRC • Select a Role and Scope

Add Cancel

User: Jacques Simon

Select a Role Business Owner

Select a Scope	New Point... Clear Favorites▼
Points	Actions
Business Line: iFinance > Investment Banking	

8. Click **Save**.
9. Enter a **Change Reason** and click **Save**.
10. Repeat this process to assign a role and scope for each user in SAS Enterprise GRC.

For more information about implementing sample data for use with the example environment, see the *SAS Enterprise GRC: Administration and Customization Guide*.

Chapter 6

Managing Financial Information

Overview	69
Overview of Financial Data Menu Options	70
Currencies	70
Exchange Rates	71
Overview of Exchange Rates	71
Example: Exchange Rate Calculation	71
Implementing Insurance Policies	72
Overview	72
Example: Creating an Insurance Policy	73

Overview

SAS Enterprise GRC provides a platform for managing and reporting a variety of different financial data as it relates to operational risk.

Most organizations have to manage financial information across a number of different international regions, and for reporting purposes tie these operational results into a standard reporting currency. SAS Enterprise GRC enables you to manage financial information across different currencies and provides methods for translating this information into other currencies through the use of exchange rates. Because exchange rates change over time, this chapter provides some information about how exchange rates affect financial items. The process of loading currency and exchange rate data is typically performed by a system administrator through a data-loading process, and is not covered in this chapter. For more information about loading currencies and exchange rates into the SAS Enterprise GRC system, see the *SAS Enterprise GRC: Administration and Customization Guide*.

In addition to currencies and exchange rates, SAS Enterprise GRC stores other financial information. For example, organizations can avoid or mitigate many operational risks through a variety of controls and processes, but not all risks can be controlled. Events both rare and regular do occur that can affect an organization financially. Organizations prepare for these loss events through the use of insurance policies to cover future losses and control gaps in coverage. This chapter provides information for a risk manager to create insurance policies manually through the SAS Enterprise GRC user interface.

Other financial information, such as financial effects from incidents, or non-insurance control costs, is reported through SAS Enterprise GRC. However, this information is

specific to the type of object and workflow. The process of entering and reporting on financial information for these objects is covered in subsequent chapters.

Overview of Financial Data Menu Options

The **Administration > Financial Data** menu enables you to perform the following tasks:



- View currencies. See “[Currencies](#)” on page 70. You must have View Currencies capability to view the Currencies window.
- View available exchange rates. See “[Exchange Rates](#)” on page 71. You must have View Exchange Rates capability to view the Exchange Rates window.
- View and manage insurance policies. See “[Implementing Insurance Policies](#)” on page 72. You must have View Insurance Policy capability to view the Insurance Policies window.

Currencies

Currencies must be data loaded. They cannot be created or edited in the Currencies window.

To view currencies, select **Administration > Financial Data > Currencies** from the menu.

Display 6.1 Example Currencies Table

Currencies			
	Description	Locale	Currency Code ▲
1	United Arab Emirates, Dirhams	DEF	AED
2	United Arab Emirates, Dirhams	en	AED
3	Emirats Arabes Unis, Dirham	fr	AED
4	الإمارات العربية المتحدة، درهم	ar	AED
5	Emirati Arabi Uniti, Dirham	it	AED
6	Emiratos Árabes Unidos, Dirham	es	AED
7	Vereinigte Arabische Emirate, Dirham	de	AED
8	Emirados Árabes Unidos, Dirhams	pt_BR	AED
9	Emirados Árabes Unidos, Dirhams	pt	AED
10	Zjednoczone Emiraty Arabskie, diram	pl	AED
  Rows 1 to 10 of 3268  			

The Currencies window contains the currency code and a description of the currency for every supported locale. Therefore, each currency code appears in the window multiple times.

Exchange Rates

Overview of Exchange Rates

Like currencies, exchange rates must be data loaded. They cannot be created or edited in the Exchange Rates window.

Objects such as losses can be reported in any currency. However, for reporting purposes the amount must be reported in the base currency. The data in the Exchange Rates table is used for the conversion. The base currency is defined in configuration options stored in the metadata. For more information about configuration of the base currency, see the *SAS Enterprise GRC: Administration and Customization Guide*.

Each exchange rate has two dates associated with it. These two dates provide the range of dates for which the rate is valid. SAS Enterprise GRC allows loading of exchange rates that have overlapping effective dates, and SAS Enterprise GRC does not perform any validation on the dates that you specify. Therefore, it is possible to load inconsistent data. For example, you can load an exchange rate of 0.784 from 1 February 2009 to 31 March 2009, and an exchange rate of 1.234 from 28 February 2009 to 10 April 2009. SAS Enterprise GRC can data load both of these exchange rates. In this case, if a user attempts to convert a currency that is dated 5 March 2009, then it will use the second exchange rate (1.234) because it is the latest exchange rate. You should be careful when loading exchange rates to avoid these types of inconsistencies.

Each exchange rate has a **From Currency** and a **To Currency** associated with it. Both currencies must match a currency code in the Currencies table. For each range of dates, you have to load only one permutation of the two currencies. For example, if you load an exchange rate of 0.500 to convert from EUR to USD, then it is not necessary to load an exchange rate of 2.000 to convert from USD to EUR. It is recommended that you load only one permutation. This practice minimizes both the amount of data and the chance of loading inconsistent data.

Example: Exchange Rate Calculation

Suppose that your base currency is USD and that a loss of 15,000 is entered in EUR on 25 March 2005. The following picture shows monthly exchange rates from January to October 2005.

Display 6.2 Example Exchange Rates

Exchange Rates					
	Exchange Rate	Effective From	Effective To	From Currency Δ	To Currency
1	1.311900	January 1, 2005 12:00:00 AM EST	February 1, 2005 12:00:00 AM EST	EUR	USD
2	1.301400	February 1, 2005 12:00:00 AM EST	March 1, 2005 12:00:00 AM EST	EUR	USD
3	1.320100	March 1, 2005 12:00:00 AM EST	April 1, 2005 12:00:00 AM EST	EUR	USD
4	1.293800	April 1, 2005 12:00:00 AM EST	May 1, 2005 12:00:00 AM EDT	EUR	USD
5	1.269400	May 1, 2005 12:00:00 AM EDT	June 1, 2005 12:00:00 AM EDT	EUR	USD
6	1.216500	June 1, 2005 12:00:00 AM EDT	July 1, 2005 12:00:00 AM EDT	EUR	USD
7	1.203700	July 1, 2005 12:00:00 AM EDT	August 1, 2005 12:00:00 AM EDT	EUR	USD
8	1.229200	August 1, 2005 12:00:00 AM EDT	September 1, 2005 12:00:00 AM EDT	EUR	USD
9	1.225600	September 1, 2005 12:00:00 AM EDT	October 1, 2005 12:00:00 AM EDT	EUR	USD
10	1.201500	October 1, 2005 12:00:00 AM EDT	November 1, 2005 12:00:00 AM EST	EUR	USD
  Rows 1 to 10 of 18  					

Because the loss occurred in March, the exchange rate of 1.32 is used. Therefore, the EUR 15,000 is converted to USD 19,800, as $15,000 \times 1.32 = 19,800$.

Implementing Insurance Policies

Overview

Insurance policies are used by incidents to mitigate losses. From the **Incident Management** menu, you can create insurance recoveries that mitigate the amount of the loss. You can also link insurance policies to risk instances from the **Risk Management** menu.

The activity status of an insurance policy is determined by the Effective Start Date and the End Date of the insurance policy. If today's date is less than the Effective Start Date or greater than the End Date, then the insurance policy is inactive. Otherwise, the insurance policy is active.

This section uses the example of Orion Star. At the company, implementing insurance policies is performed by insurance policy officers.

Example: Creating an Insurance Policy

Robert Fitzgerald, the Risk Manager for the Securities Department, has the additional role of an insurance policy officer, and is responsible for creating new insurance policies. Robert has purchased an insurance policy for his department to recoup any losses as the result of theft to local property in the United States. Theft does not include fire damage.

The policy has the following attributes:

Policy Attribute	Value
Operational area	Management organization: Securities for Investment Banking division Geography: United States
Policy number	9999-9999-01
Policy type	Internal
Used in the capital calculation?	No
Date acquired	September 2, 2010
Effective start date	September 15, 2010
Effective end date	September 15, 2011
Cancellation notice period	30 days
Coverages	Theft
Exclusions	None
Warranties	None
Currency for coverage	EUR
Insured value	2000000
Deductible	20000
Individual Limit	2000000
Aggregate Limit	4000000
Currency for Payment	EUR
Premium (Without Taxes)	1950

Policy Attribute	Value
Premium	2000
Total Annual Cost	24000
Insurance Company	Travelers
Insurer ECAI 1	Standard & Poor's
Insurer Credit Score 1	AA+
Insurer ECAI 2	Moody's
Insurer Credit Score 2	Aa1

To create an insurance policy, complete these steps as Robert:

1. Log on to SAS Enterprise GRC.
2. Select **Administration > Financial Data > Insurance Policies** from the menu. The Insurance Policies window appears.
3. Click **Create Insurance Policy**. The Create Insurance Policy window appears.
4. Select the operational area for the issue. Click **Edit**. In the Operational Area window, select the following dimensions and nodes from the Dimension drop-down list and click **Add** for each.
 - Dimension: **Management Organization**
Node: **Management Organizations > iFinance > Investment Banking > Securities**
 - Dimension: **Geography**
Node: **Geographies > Americas > North America > United States**

Click **OK** to add the operational area and return to the Create Insurance Policy window.
5. On the **Details** tab, enter the summary details about the policy:
 - a. Enter the policy number *9999-9999-01* in the **Policy Number** field.
 - b. Enter *Local Property and Liability Insurance Program* in the **Name** field.
 - c. Enter *Insurance for local property in the Securities Department* in the **Description** field.
 - d. The policy is internal. Select the policy as **Internal** in the **Policy Type** drop-down list.
 - e. Select whether to include the insurance policy in the **Use in Capital Calculation** field.
 - f. In the **Date Acquired** field, choose *September 2, 2010*.
 - g. In the **Effective Start Date** field, choose *September 15, 2010*.
 - h. In the **End Date** field, choose *September 15, 2011*. The insurance policy is inactive after this date.

- i. In the **Cancellation Notice Period (Days)** field, enter 30.
 - j. Click **Edit** to provide the types of protection this policy covers in the **Coverages** field. Select **Theft**.
 - k. Click **Edit** to provide information about the types of protection that this policy does not cover in the **Exclusions** field (for example, external fraud).
 - l. Click **Edit** to provide any warranty information in the **Warranties** field.
6. On the **Coverage Amounts** tab, enter the coverage amount information:
 - a. In the **Currency for Coverage** drop-down list, select **EUR**.
 - b. In the **Deductible** field, enter 20000.
 - c. In the **Individual Limit** field, enter 2000000.
 - d. In the **Aggregate Limit** field, enter 4000000.
7. On the **Insurance Policy Costs** tab, enter the policy costs:
 - a. In the **Currency for Payment** field, select **EUR**.
 - b. In the **Premium (Without Taxes)** field, enter 1950.
 - c. In the **Premium** field, enter 2000.
 - d. In the **Payment Frequency** field, select **Monthly**.
 - e. In the **Total Annual Cost** field, enter 24000.
8. On the **Insurers** tab, enter the insurer information:
 - a. In the **Insurance Company** field, select **Travelers**.
 - b. In the **Insurer ECAI 1** field, select **Standard and Poor's**.
 - c. In the **Insurer Credit Score 1** field, select **AA+**.
 - d. In the **Insurer ECAI 2**, select **Moody's**.
 - e. In the **Insurer Credit Score 2** field, select **Aa1**.
9. Leave the defaults for other fields, and click **Save** to save the policy.

Chapter 7

Managing Organizational Policies

Overview	77
Policies and Policy Workflows	78
Overview	78
Roles for Policy Management	79
Policy Lifecycle	80
Implementing an Example Policy	81
Example Policy Management Process	81
Example: Policy Administrator Creates the Policy	83
Example: IT Policy Approver Reviews and Approves the Policy	84
Example: Policy Administrator Requests Responses	84
Example: Respondent Provides a Policy Response	85
Example: Policy Administrator Marks Policy as Communicated	85
Example: Policy Administrator Expires Policy	85
Example: IT Policy Approver Expires Policy	85

Overview

In SAS Enterprise GRC, *policies* refer to rules or guidelines that govern how an organization executes its operations. The objective of policy management is to define policies for the organization and manage their lifecycle.

Specifically, policies are designed to meet certain regulatory obligations and organizational objectives. Policies can also be associated with a variety of business objects, such as incidents, risks, or controls, to ensure that a policy is operationally effective.

For example, an organization might have a policy that defines how its computer systems can be used to conduct business. The use of personal e-mail might be disallowed or discouraged. This policy is intended to decrease the amount of Web traffic and lower the risk of infection by computer worms. Thus, a policy can tie into risk mitigation by reducing the probability of a computer worm and also serve to meet an organizational objective to reduce employee Internet traffic use by 10%.

Lifecycle management is achieved through workflow stages. The following workflow stages exist by default:

- Create
 - The policy is created and saved, then sent for approval.
- Approve

The policy is approved by one or more policy approvers.

- Communicate

The policy is sent to the appropriate policy respondents (employees that will be impacted by the new or updated policy) and as necessary, policy respondents indicate they have read and understood the policy and will comply with it. Following this, the policy is considered communicated to the organization.

- Monitor

The policy is maintained until it is expired, or until it is no longer effective.

- Approve Policy Expiration

The policy expiration is approved by one or more policy approvers.

- Expired

The policy is no longer effective.

The policy management workflow enables accountability and creates a traceable information stream for auditing and reporting purposes.

By default, there are three types of policies: human resources (HR) policies, information technology (IT) policies, and sales policies. The type of policy governs the workflow used to approve the policy. For example, an HR policy must be approved both by legal and HR, whereas an IT policy only requires IT approval, and so on.

Note: These are only examples of the types of policies available by default. Policy types and workflows are customizable.

This chapter is primarily intended for users who participate in policy creation and management and enter data by means of the graphical user interface. For more information about the roles that participate in the policy management process, see [“Roles for Policy Management” on page 79](#).

This chapter uses the example of Orion Star, a bank that is using SAS Enterprise GRC to manage its GRC activities, and that wants to administer policies through the system. The example uses the default SAS Enterprise GRC user interface environment, and assumes you have completed steps in previous chapters to implement the business structure, assign users to roles, and so on. It also assumes that you understand the workflows for managing policies for this example. For more information about this example, see [Chapter 3, “Gathering Governance, Risk, and Compliance Data,” on page 27](#).

For more information about the default policy management workflows, see the *SAS Enterprise GRC: Administration and Customization Guide*.

Policies and Policy Workflows

Overview

SAS Enterprise GRC enables the process of managing policies through the **Policy Management** menu. This menu enables you to perform the following tasks:

- Manage policies through the **Policies** submenu.

You must have Policy capabilities assigned to manage the **Policies** submenu.

- Manage policy responses through the **Policy Responses** submenu. You can use this area to review policy responses and respond to policies.

You must have Policy Response capabilities assigned to manage the **Policy Responses** submenu.

The management of policy workflows is completed through SAS Workflow Studio. For more information about policy workflows and using the SAS Workflow Studio, see the *SAS Enterprise GRC: Administration and Customization Guide*.

Roles for Policy Management

Capabilities to manage policies are assigned through roles. The following table describes each role as it pertains to policy management.

Table 7.1 Roles for Policy Management

Role	Description
Enterprise GRC: Administration	Administrator. Administers the SAS Enterprise GRC environment. Might have responsibilities for maintaining policy workflows.
Enterprise GRC: Policy Administration	Policy Administrator. Responsible for the creation, ownership, and administration of policies. Has responsibilities for creating processes, obligations, and objectives that link to a policy.
Enterprise GRC: IT Policy Approval	IT Policy Approver. Responsible for approving IT policies.
Enterprise GRC: Human Resources Management	HR Policy Approver. Responsible for approving HR policies.
Enterprise GRC: Policy Approval	Sales Policy Approver. Responsible for approving Sales policies.
Enterprise GRC: Legal Counsel	Sales and HR Policy Approver. Responsible for approving both HR and Sales policies.
Policy Owner	Responsible for the policy. Although there is no default SAS Enterprise GRC role for this person, a policy owner must have the Create and Update capabilities for policies and the Create capability for policy responses. This person is not necessarily the person who initiates or performs actions on a policy, but is typically a policy administrator or central risk manager.
Policy Respondent	Responsible for responding to a policy when assigned. Although there is no default SAS Enterprise GRC role for this person, a policy respondent must have the Update capability for Policy Response in the exact operational location of the policy in order to respond to policies. For example, if you have a policy that applies to a child organization and you have Policy Response capabilities only in the parent organization, you will not be able to respond to policies that apply to the child organization.

Note: Depending on the capabilities of your assigned role, certain objects and fields in the user interface might be disabled for you during the completion of a task.

Policy Lifecycle

The default policy management lifecycle is completed using the following steps:

1. The Administrator works with the Policy Administrator to initially define the policy workflow using SAS Workflow Studio. For more information about managing and customizing the policy management workflow, see the *SAS Enterprise GRC: Administration and Customization Guide*.
2. The Policy Administrator initially defines any linkable policy-related business objects. A number of business objects, such as controls, risks, and issues, can be linked to the policy. In particular, the following business objects are often linked to policies:
 - processes
 - obligations
 - objectives

For more information about creating processes, obligations, and objectives, see [“Implementing the Business Structure” on page 49](#).

3. The Policy Administrator creates the policy and provides details about the policy.

Depending on the management organization and the type of policy, the policy is then assigned to one or more Policy Approvers. The Policy Administrator also assigns the Policy Owner and one or more Policy Administrators and Policy Respondents.

The Policy Administrator has the option to link the policy to other business objects, attach files or links, or add comments. The Policy Administrator then sends the policy for approval.

4. One or more Policy Approvers approve the policy, depending on the policy type.
5. The Policy Administrator requests responses to the policy from one or more Policy Respondents.
6. Policy Respondents submit their responses to the policy. Respondents can accept compliance with the policy or state exceptions or other reasons for not complying with the policy.
7. If any respondents do not accept full compliance with the policy, the Policy Administrator must approve the response. If rejected, the respondent must change their response.
8. The Policy Administrator reviews the responses and signs off to indicate that policy communication has been completed.

Note: The Policy Administrator has the option to note the communication of a policy without sending the policy for response or requiring completed policy responses.

9. The policy is monitored for changes and is periodically reviewed. Review dates can be set on the policy to notify the Policy Administrator before the next review.
10. The policy is expired either by the effective end date of the policy, or by the Policy Administrator. Policy expiration requires approval by Policy Approvers (again, depending on the type of policy). After it is approved by all approvers, the policy is considered frozen at the time of the expiration.

Note: Business objects linked to the policy can display changes made after policy expiration.

11. New versions of the original policy can be created from old policies, even after policy expiration. By default, policies with the same policy name must have a unique version.

Implementing an Example Policy

Example Policy Management Process

The Investment Banking division at Orion Star is rolling out their GRC infrastructure, and is implementing a number of corporate policies that govern how the division conducts business. For the purpose of this example, the following table displays the users involved in policy administration. The responsibilities and roles that you define vary depending on your organization.

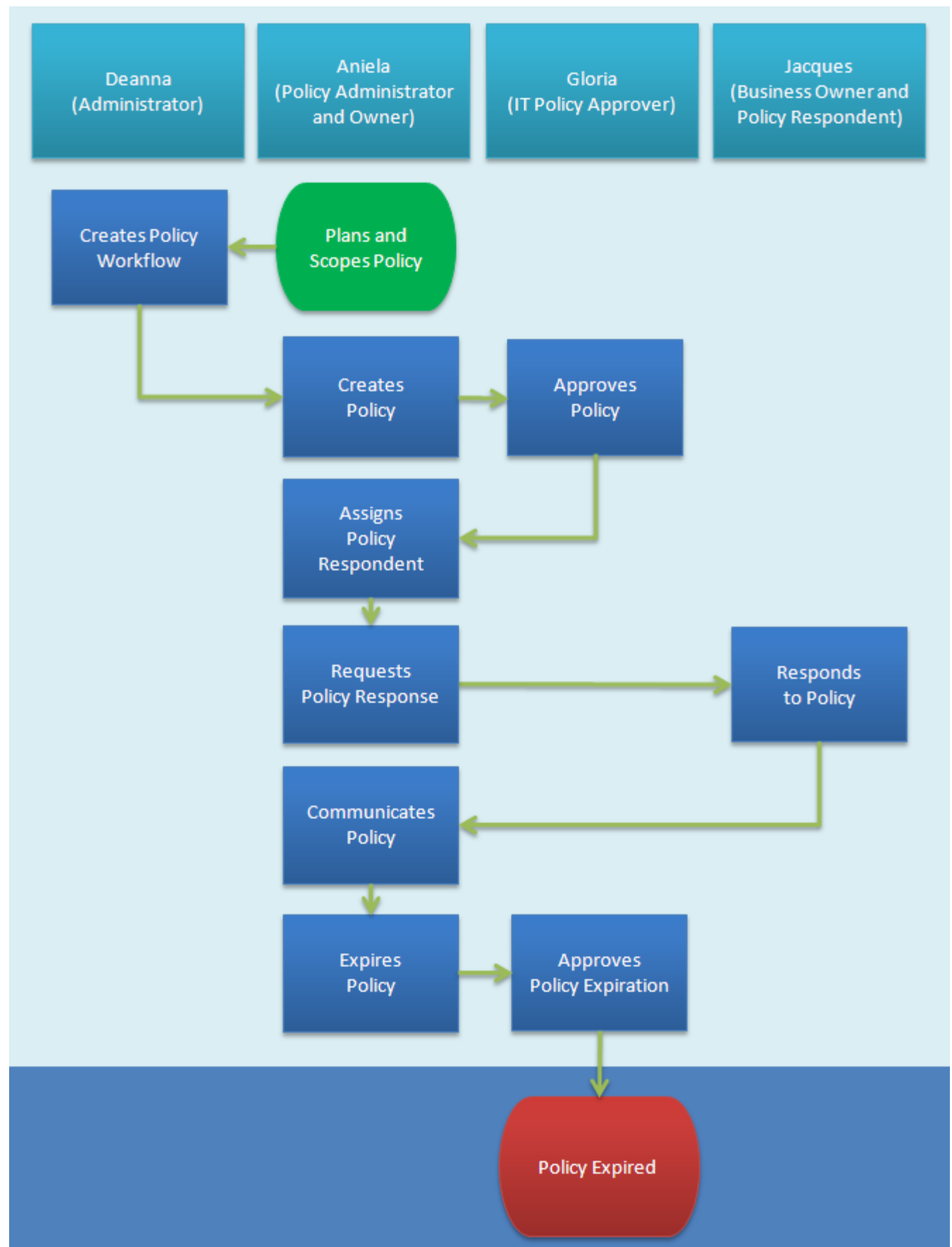
User	Job Title	SAS Enterprise GRC Roles
Deanna Tiswell	Administrator	Enterprise GRC: Administration
Aniela Olesky	Investment Banking Policy Administrator	Enterprise GRC: Policy Administration
Gloria Hyatt	Investment Banking Division Expert	Enterprise GRC: IT Policy Approval
Jacques Simon	Central Operational Risk Manager, Investment Banking	Enterprise GRC: Business Ownership (Respondent)

Last year, an e-mail virus initiated by an employee who opened an e-mail attachment resulted in the downtime of several large server farms that control the Investment Banking division's trading activities. In order to reduce the risk of future downtime, and as part of a corporate objective to reduce costs pertaining to bandwidth use, the Investment Banking division at Orion Star is implementing an IT policy that discourages the use of personal e-mail at work. A policy documentation expert has drafted the policy, and the division now needs to implement the policy.

This specific example assumes that Jacques accepts the policy as written, and that the default workflow processes are in place.

The following figure describes the process for the example of Orion Star.

Display 7.1 Policy Workflow for Orion Star



The example follows these steps:

1. Aniela, the Policy Administrator, [creates the policy](#).
2. Gloria, the Investment Banking Division Expert, [reviews and approves the policy](#).
3. Aniela, the Policy Administrator, [sends a response request to Jacques](#).
4. Jacques, the Central Operational Risk Manager, [responds to and accepts the policy](#).
5. Aniela [marks the policy as communicated](#).
6. When the policy no longer applies, Aniela [marks the policy as expired](#).
7. Gloria, the Investment Banking Division Expert, [approves the policy expiration](#).

Example: Policy Administrator Creates the Policy

Aniela creates a new policy as Policy Administrator. Complete these steps as Aniela:

1. Select **Policies > Policies** from the menu. The Policies window appears.
2. Click **Create Policy**. The Create Policy window appears.
3. On the **Details** tab, enter the details of the policy:
 - a. Select the operational area for the policy. In the OL chooser, click **Edit** and in the Operational Area window, select the following dimensions and nodes from the Dimension drop-down list, and click **Add** for each.
 - Dimension: **Management Organization**
 Node: **Management Organizations > iFinance > Investment Banking**
 Click **OK** to add the operational area and return to the previous window.
 - b. Enter *E-mail use IT policy* for the **Policy Title**.
 - c. Keep the default, *1.0*, for the **Policy Version**.
 - d. Select **Information Technology** as the **Policy Type**. The approval workflow is dependent on the policy type.
 - e. Enter *Policy to discourage external e-mail use.* as the **Policy Description**.
 - f. Enter *Policy aimed at reducing e-mail viruses and Web use.* as the **Policy Objective**.
 - g. Select the dates for which the policy is effective. Provide an appropriate start date in the **Effective From Date** and an appropriate end date in the **Effective To Date** fields. Also provide a due date for the review in the **Next Review Date** field, which must be between the start and end dates.
 - h. Select **Standard Policy Responses** in the **Response Values List** drop-down list.
 - i. Select **No** for **Is Training Required**.
 - j. Expand **Related Costs**. In the Costs table, click **Create Cost**. The Create Cost window appears.
 - k. Enter *Documentation fees* as the **Description**.
 - l. Select **Documentation costs** in the **Cost Type** field.
 - m. The fees for writing a policy draft were \$2500. Enter *2500* as the **Cost Amount** and select **USD** in the currency drop down. Click **OK** to close the Create Cost window.

4. On the **Resources** tab, complete these steps:
 - a. Aniela is both the Policy Owner and Policy Administrator. In the Policy Administrators table, click **Link Policy Administrators** and select Aniela. Click **Add and Close**.
 - b. View the Information Technology Approvers. Gloria should appear as one of the approvers.
5. On the **Related Content** tab, link the policy to an objective. This assumes you have already created an objective that ties into the policy. For more information about creating the sample objective, see [“Example: Creating an Objective Instance” on page 62](#).
6. The example assumes that no attachments are needed for the policy. However, you can click the **Attachments** tab should the policy exist in another document format.
7. Click **Apply** to apply changes to the policy.
8. Click **Send for Approval**, enter a **Change Reason**, and click **Save** to send the policy to the Information Technology Approver.
9. Log off from SAS Enterprise GRC.

Example: IT Policy Approver Reviews and Approves the Policy

Gloria approves the new policy as IT Policy Approver. Complete these steps as Gloria:

1. Select **Policies > Policies** from the menu. The Policies window appears.
2. Click the E-mail use IT policy. The View Policy window appears.
3. Review the details of the policy. Gloria is satisfied that the new policy covers all criteria. Click **Approve**, enter a **Change Reason**, and click **Save**. The Policy Administrator is notified that the policy has been approved.
4. Log off from SAS Enterprise GRC.

Example: Policy Administrator Requests Responses

Aniela, as Policy Administrator, requests a response from Jacques. Complete these steps as Aniela:

1. Select **Policies > Policies** from the menu. The Policies window appears.
2. Click the E-mail use IT policy. The Edit Policy window appears.
3. On the **Respondents** tab, select the respondent. In the Respondents table, click **Add Users** and select Jacques as the policy respondent. You can send response requests to individuals or all at once.
4. Click **Request Responses**, which sends a response request to all respondents. In this case, only Jacques is a respondent.
5. Log off from SAS Enterprise GRC.

Example: Respondent Provides a Policy Response

Jacques, as Policy Respondent, notes compliance to the policy. Complete these steps as Jacques:

1. Select **Policies > Policy Responses** from the menu. The Policy Responses window appears.
2. Click on the policy response for the E-mail use IT policy. The Edit Policy Response window appears.
3. Jacques reviews the policy and accepts the policy. On the **Details** tab, select **Accept** as the **Response**.
4. Enter *This will help us meet our risk and cost reduction goals.* as the **Justification**.
5. Click **Submit Response** to send the response to the Policy Administrator.
6. Log off from SAS Enterprise GRC.

Example: Policy Administrator Marks Policy as Communicated

Aniela, as Policy Administrator, reviews the response and marks the policy as communicated. Complete these steps as Aniela:

1. Select **Policies > Policies** from the menu. The Policies window appears.
2. Click on the policy for the E-mail use IT policy. The Edit Policy window appears.
3. Aniela reviews the response in the **Respondents** tab and marks the policy as communicated. Click **Communicate Policy Complete**.
4. Log off from SAS Enterprise GRC.

Example: Policy Administrator Expires Policy

Aniela, as Policy Administrator, decides the policy should be expired, to make way for the creation of a new version of the IT use policy. Complete these steps as Aniela:

1. Select **Policies > Policies** from the menu. The Policies window appears.
2. Click on the policy for the E-mail use IT policy. The Edit Policy window appears.
3. Aniela submits the policy expiration for approval. Click **Expire Policy Now**, enter a **Change Reason**, and click **Save**. The policy expiration goes to Gloria for approval.
4. Log off from SAS Enterprise GRC.

Example: IT Policy Approver Expires Policy

Gloria, as IT Policy Approver, approves the policy expiration. Complete these steps as Gloria:

1. Select **Policies > Policies** from the menu. The Policies window appears.
2. Click on the policy for the E-mail use IT policy. The Edit Policy window appears.

3. Gloria reviews the policy history and justification for expiring the policy, and approves the policy expiration. Click **Approve**, enter a **Change Reason**, and click **Save**. The policy is now expired.
4. Log off from SAS Enterprise GRC.

Chapter 8

Implementing Issues and Action Plans

Overview	87
Implementing Issues and Action Plans	88
Overview	88
Roles for Issues and Action Plans	88
Issues and Action Plan Lifecycle	89
Implementing an Example Issue and Action Plan	91
Example Issue and Action Plan Process	91
Example: Issue Originator Creates the Issue	93
Example: Issue Approver Reviews and Approves the Issue	94
Example: Issue Owner Accepts the Issue and Develops an Action Plan	94
Example: Action Plan Approver Reviews and Approves the Action Plan	95
Example: Action Plan Owner Completes the Action Plan	95
Example: Action Plan Approver Reviews and Approves the Action Plan Completion	95
Example: Action Plan Originator Approves the Action Plan Closure	96
Example: Issue Owner Ends Issue Modification and Closes the Issue	96
Example: Issue Approver Reviews and Approves the Issue Closure	96

Overview

In risk management, *issues* are defined as items that require a change that would remove the issue, mitigate the issue, or both. *Action plans* are typically developed to mitigate or respond to issues, although they might be standalone tasks or tasks created in response to other types of events.

Before a user can properly administer issues, a system administrator must first create an environment suitable for investigating and responding to issues. Typically this requires implementing the organization's business structure, assigning roles and responsibilities to users, and setting up the appropriate exchange rates and currencies for use in the Web application. See the preceding chapters for information about implementing these environmental characteristics.

The lifecycle management of issues and action plans is achieved through workflow stages. This workflow enables accountability and creates a traceable information stream for auditing and reporting purposes. Issues and action plans have separate workflows, but these workflows are integrated.

This chapter uses the example of Orion Star, a bank that is using SAS Enterprise GRC to manage its GRC activities. The example uses the default SAS Enterprise GRC user

interface environment, and assumes that data has already been gathered about issues, that users have been assigned to the appropriate roles, and that action plans are either developed or are in development. Your environment might vary depending on the level of customization. For more information about this example, see [Chapter 3, “Gathering Governance, Risk, and Compliance Data,”](#) on page 27.

For more information about the default issue and action plan workflows, see the *SAS Enterprise GRC: Administration and Customization Guide*.

Implementing Issues and Action Plans

Overview

SAS Enterprise GRC enables the process of creating issues and developing action plans through the **Issues and Action Plans** menu. This menu enables you to perform the following tasks:

- Manage issues. You must have View Issue capability to view the **Issues** menu.
- Manage action plans. You must have View Action Plan capability to view the **Action Plans** menu.

Issues and action plans are related to each other. Most action plans are created in response to an issue, although action plans can be created independently of an issue. You can also create an action plan in response to multiple issues, or create multiple action plans to respond to an issue.

Issue and action plan approval workflows use SAS Workflow Studio, but some workflow stages contain static workflow content. For more information about managing workflows and using the SAS Workflow Studio for dynamic workflow content, see the *SAS Enterprise GRC: Administration and Customization Guide*.

Roles for Issues and Action Plans

Capabilities to manage issues and action plans are assigned through roles. The following table describes each role as it pertains to issues and action plans.

Table 8.1 Roles for Issues and Action Plans

Role	Description
Enterprise GRC: Administration	Administrator. Administers the SAS Enterprise GRC environment. Might have responsibilities for maintaining issue and action plan workflows.
Issue Originator	Responsible for creating the issue. Although there is no default SAS Enterprise GRC role for this person, an issue originator must have the Create and Update capabilities for issues. This person is not necessarily the person who owns the issue, but recognizes the issue and assigns it to the appropriate owner. Issue origination can be performed by a number of SAS Enterprise GRC roles.

Role	Description
Enterprise GRC: Issue Ownership	Issue Owner. Responsible for owning issues. Can also be responsible for creating issues.
Enterprise GRC: Issue Approval	Issue Approver. Responsible for approving issues.
Action Plan Originator	Responsible for creating the action plan. Although there is no default SAS Enterprise GRC role for this person, an action plan originator must have the Create and Update capabilities for action plans. This person is not necessarily the person who owns the action plan, but creates the action plan and assigns it to the appropriate owner. Action plan origination can be performed by a number of SAS Enterprise GRC roles.
Enterprise GRC: Action Plan Ownership	Action Plan Owner. Responsible for owning action plans. Can also be responsible for creating action plans.
Enterprise GRC: Action Plan Approval	Action Plan Approver. Responsible for approving action plans.

Note: Depending on the capabilities of your assigned role, certain objects and fields in the user interface might be disabled for you during the completion of a task.

Because action plans are often created in response to an issue, either the Issue Originator or the Issue Owner is usually the same user as the Action Plan Originator. In fact, it is possible for a single user to perform the tasks of all four roles. It is also possible for each task to be performed by a different user. In any case, the Issue Owner is ultimately responsible for giving final approval on closing an action plan if that action plan was created out of an issue.

Issues can also be created or linked from key risk indicators (KRIs) or automatically generated through the form-based assessment process or the triggering of an *issue threshold*. Issue thresholds are closely associated with the incident management process. For more information about issue thresholds, see [“Incident Investigation – Issue Thresholds” on page 176](#).

Issues and Action Plan Lifecycle

After the Administrator has properly set up all issue and action plan workflows as needed, the issue and action plan lifecycle can begin.

The Issue process is completed using these steps:

1. The Issue Originator creates the issue and saves it as a draft. The Issue Originator also assigns an Issue Owner. The Issue Originator then publishes the draft, which is sent for approval.
2. The Issue Approver reviews and approves the issue.
3. The Issue Owner accepts the issue.
4. The Issue Owner closes the issue, which is sent for approval.

Note: Any action plans within the issue must be closed or deleted before the issue can be closed.

5. The Issue Approver approves issue closure. The issue is now closed.

The Action Plan process is completed using the following steps:

1. The Action Plan Originator creates the action plan, links it to an issue as necessary, and saves it as a draft.
2. The Action Plan Originator publishes the action plan, which is sent for approval.
3. The Action Plan Approver approves the action plan.
4. The Action Plan Owner accepts the action plan.
5. The Action Plan Owner completes the action plan, which is sent for approval.
6. The Action Plan Approver approves the action plan pending completion approval. The action plan is now completed.
7. The Action Plan Originator approves the completed action plan. If approved, the action plan is now closed.

The following actions can also be taken during the lifecycle:

- An Open or Pending issue can be reassigned to a different owner.
Whenever an Issue Owner is reassigned, the status of the issue becomes Open. Any action plans linked to the issue are not affected by the reassignment.
- An Open, Pending, or Completed action plan can be reassigned to a different owner.
Whenever an Action Plan Owner is reassigned, the status of the action plan becomes Open. Any issues linked to the action plan are not affected by the reassignment.
- A Completed action plan can be rejected by the Action Plan Originator.
When a completed action plan is rejected, the status of the action plan becomes Open.
- If the Issue Originator and the Issue Owner are the same user, then the issue skips the issue acceptance stage.
- If the Action Plan Originator and the Action Plan Owner are the same user, then the action plan skips the action plan acceptance stage.
- An issue pending approval by an Issue Approver is read-only.
- An action plan pending approval by an Action Plan Approver is read-only.
- An Open or Pending issue can be deleted.
The status of the issue becomes Canceled. The cancellation must be approved by the Issue Approver.
- An Open, Pending, or Completed action plan can be deleted.
The status of the action plan becomes Canceled. The cancellation must be approved by the Action Plan Approver.
- A Draft issue or action plan can be deleted.
The issue or action plan is permanently removed from the system.

Implementing an Example Issue and Action Plan

Example Issue and Action Plan Process

The Investment Banking division at Orion Star is working on a fraud event that exceeded \$10,000. The loss resulted from a process gap in which accountants did not produce and review financial reports and statements. This loss triggered an internal investigation, the result of which is an action plan to train accountants on producing financial reports and statements. (SAS Enterprise GRC can also automatically trigger issue creation through incident management. But, for the purposes of this example, assume that incident management is not used.)

For the purpose of this example, the following table displays the users involved in working with the example issue and action plan.

Table 8.2 Example Issue and Action Plan Users and Roles

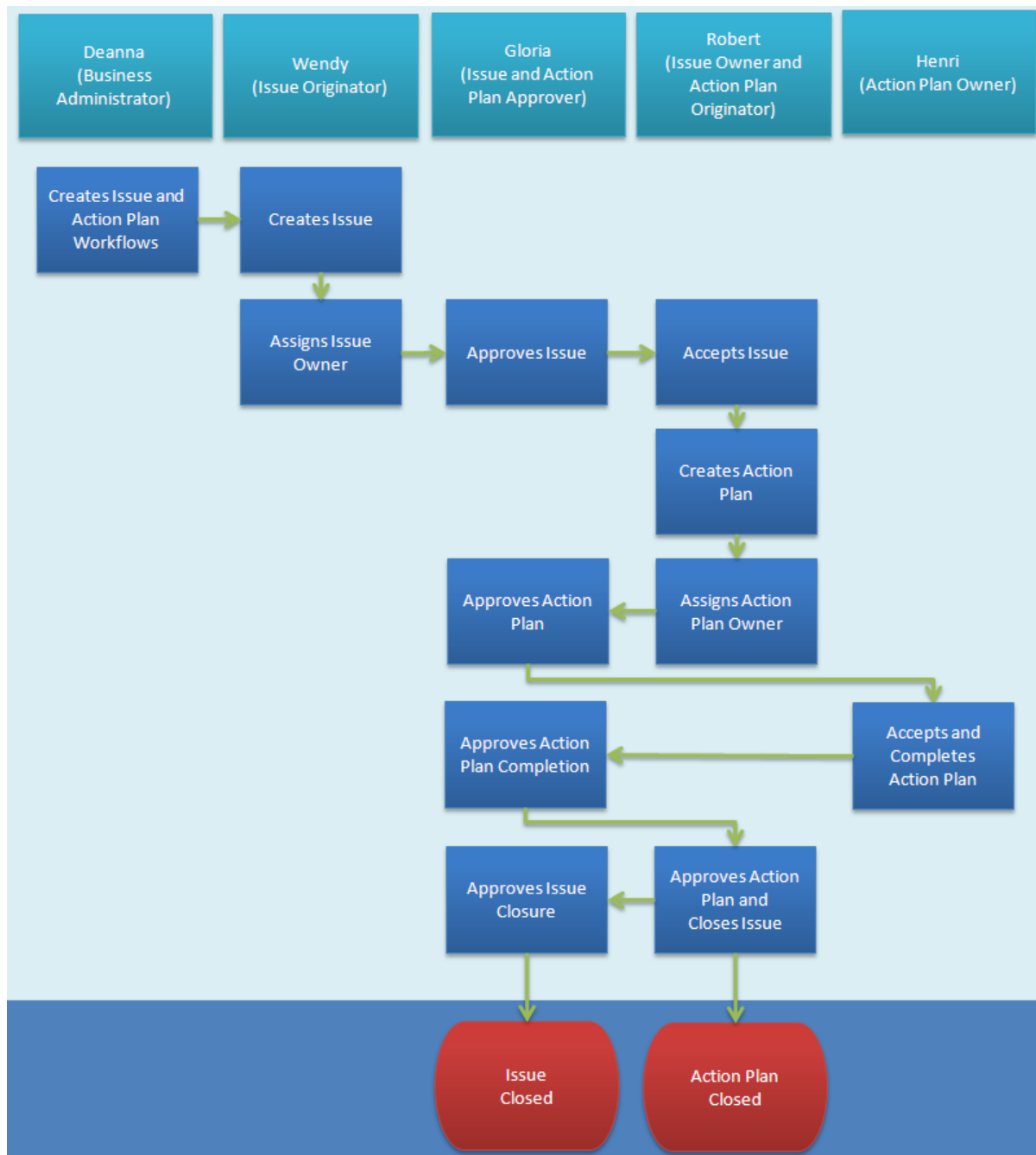
User	Job Title	SAS Enterprise GRC Roles
Wendy Feinstein	Securities Department Investigator	Enterprise GRC: Incident Investigation (Issue Originator)
Gloria Hyatt	Investment Banking Division Expert	Enterprise GRC: Issue Approval Enterprise GRC: Action Plan Approval
Robert Fitzgerald	Securities Department Risk Manager	Enterprise GRC: Issue Ownership Enterprise GRC: Local Business Management (Action Plan Originator)
Henri LeBlanc	Risk Project Manager	Enterprise GRC: Action Plan Ownership

In our example, Wendy Feinstein, a Securities Department Investigator in the Investment Banking Division, is the Incident Investigator (and therefore an Issue Originator). Robert Fitzgerald, the Securities Department Risk Manager, is both the Issue Owner and Action Plan Originator, and Henri LeBlanc, the Risk Project Manager, is the Action Plan Owner. Gloria is the department expert responsible for approving issues and action plans.

Wendy creates the issue in SAS Enterprise GRC. Robert, the Risk Manager for the Securities Department, inherits the issue and develops a corresponding action plan in his dual role as Issue Owner and Action Plan Originator. The action plan is then assigned to Henri, who is responsible for the development of a course to train employees on financial report creation that is estimated to cost USD 2,000. The actual cost of the training course is USD 2,500. Upon completion of the training, Henri reports its completion to Robert, who considers the issue closed.

The following figure describes the process for the example of Orion Star.

Display 8.1 Issues and Action Plans Workflow




The example follows these steps:

1. Wendy, the Securities Department Investigator, creates the issue and assigns it to Robert.
2. Gloria, the Investment Banking Division Expert, reviews and approves the issue.
3. Robert, the Securities Department Risk Manager, accepts the issue, develops an action plan, and assigns it to Henri.
4. Gloria reviews and approves the action plan.

5. Henri **completes the action plan**.
6. Gloria **reviews and approves the completed action plan**.
7. Robert **approves the action plan closure**.
8. Robert **ends modification of the issue, and marks the issue closed**.
9. Gloria **approves the issue closure**.


Example: Issue Originator Creates the Issue

Wendy creates the issue as Issue Originator. Complete these steps as Wendy:

1. Select **Issues and Action Plans > Issues** from the menu. The Issues window appears.
2. Click **Create Issue**. The Create Issue window appears.
3. Select the operational area for the issue. In the OL chooser, click the Edit icon (). In the New Operational Point window, select the following dimensions and nodes from the Dimension drop-down list and click **Add** for each.

- Dimension: **Management Organization**
Node: **Management Organizations > iFinance > Investment Banking > Securities**
- Dimension: **Process Type**
Node: **Processes > Support > Accounting > Produce financial reports and statements**
- Dimension: **Geography**
Node: **Geographies > Americas > North America > United States**

Click **Add and Close** to add the operational point and return to the previous window.

4. Enter the details of the issue:
 - a. Enter *Accounting process gap for producing reports* in the **Title** field.
 - b. Enter the description of the issue, such as *Accounting department did not produce financial reports*, in the **Description** field.
 - c. Because this type of issue is considered a high priority by the risk management team, select **High** in the **Priority** field.
 - d. Enter a future date (for example, 12 December 2012) in the **Target Completion Date** field.
 - e. In the **Issue Owner** field, click on the Select User icon (). Select **Robert Fitzgerald** as the issue owner.
5. Accept the defaults for the remaining fields. Click **Save as Draft**.
6. Click **Send for Publish Approval**, enter a **Change Reason**, and click **Save**. The issue is sent to the Issue Approver for approval.
7. Log off from SAS Enterprise GRC.

Example: Issue Approver Reviews and Approves the Issue

Gloria approves the new issue as Issue Approver. Complete these steps as Gloria:


1. Select **Issues and Action Plans > Issues** from the menu. The Issues window appears.
2. Click on the accounting process gap issue. The View Issue window appears.
3. Review the details of the issue. Gloria is satisfied with the issue as reported. Click **Publish Approved**, enter a **Change Reason**, and click **Save**. The Issue Owner is notified that the issue has been approved.
4. Log off from SAS Enterprise GRC.

Example: Issue Owner Accepts the Issue and Develops an Action Plan

Robert accepts the new issue as Issue Owner. Complete these steps as Robert:

1. Select **Issues and Action Plans > Issues** from the menu. The Issues window appears.
2. Click on the accounting process gap issue. The View Issue window appears.
3. Review the details of the issue. Click **Accept**, and then click **Done**.

After the issue is accepted, Robert can develop an action plan for the issue. Complete these steps as Robert:

1. On the View Issue window, click **Begin Modification**. The **Edit Issue** window appears.
2. In the **Action Plans** table, click **Create**. The Create Action Plan window appears.
3. Enter the details of the action plan in the **Details** section. Complete these steps:
 - a. Enter *Financial Reporting Training Course* in the **Title** field.
 - b. Enter the description of the action plan in the **Description** field.
 - c. Because this action plan is considered a high priority by the risk management team, select **High** in the **Priority** field.
 - d. Enter a future date (for example, 01 December 2012) in the **Target Completion Date** field. The date for completing an action plan should be a date before the target completion date of the issue.
 - e. In the **Owner** field, click on the Select User icon (). Select **Henri LeBlanc** as the action plan owner.
4. Expand **Action Plan Costs**. Enter the action plan costs in the **Action Plan Costs** section. Complete these steps:
 - a. Enter *Mitigates future fraud* in the **Control Improvement Potential** field.
 - b. The estimated cost of the training program was \$2000. Enter *2000* in the **Estimated Cost or Budget Amount** field. Select **USD** as the **Estimated Cost Currency**.
 - c. The actual cost of the training program was \$2500. Enter *2500* in the **Actual Cost Amount** field. Select **USD** as the **Estimated Cost Currency**.

5. Accept the defaults for the remaining fields. Click **Save as Draft**.
6. Click **Send for Publish Approval**, enter a **Change Reason**, and click **Save**. The action plan is sent to the Action Plan Approver for approval.
7. Log off from SAS Enterprise GRC.

Example: Action Plan Approver Reviews and Approves the Action Plan

Gloria approves the action plan as Action Plan Approver. Complete these steps as Gloria:

1. Select **Issues and Action Plans > Action Plans** from the menu. The Action Plans window appears.
2. Click on the financial reporting training course action plan. The View Action Plan window appears.
3. Review the details of the action plan. Gloria is satisfied with the action plan as reported. Click **Publish Approved**, enter a **Change Reason**, and click **Save**. The Action Plan Owner is notified that the action plan has been approved.
4. Log off from SAS Enterprise GRC.

Example: Action Plan Owner Completes the Action Plan

Henri accepts and completes the action plan. Complete these steps as Henri:

1. Select **Issues and Action Plans > Action Plans** from the menu. The Action Plans window appears.
2. Click on the financial training action plan. The View Action Plan window appears.
3. Review the details of the action plan. Click **Accept**, and then click **Done**.

After the action plan is accepted, Henri completes the action plan. Complete these steps as Henri:

1. On the **Issues and Action Plans** tab, click on the **Action Plans** subtab. The Action Plans window appears.
2. In the View Action Plan window, click **Send for Complete Approval**, enter a **Change Reason**, and click **Save**. The action plan is sent to the Action Plan Approver for approval.

Example: Action Plan Approver Reviews and Approves the Action Plan Completion

Gloria approves the completed action plan. Complete these steps as Gloria:

1. Select **Issues and Action Plans > Action Plans** from the menu. The Action Plans window appears.
2. Click on the financial training action plan. The View Action Plan window appears.
3. Review the details of the action plan. Gloria accepts the action plan as completed. Click **Completion Approved**, enter a **Change Reason**, and then click **Save**.

Example: Action Plan Originator Approves the Action Plan Closure

Robert approves the completed action plan as Action Plan Originator. Complete these steps as Robert:

1. Select **Issues and Action Plans > Action Plans** from the menu. The Action Plans window appears.
2. Click on the financial training action plan. The View Action Plan window appears.
3. Review the details of the action plan. Robert accepts the action plan as completed, and closes the action plan. Click **Approve**. The action plan is now closed.

Example: Issue Owner Ends Issue Modification and Closes the Issue

With the action plan completed, Robert ends modification of the issue as Issue Owner. Complete these steps as Robert:

1. Select **Issues and Action Plans > Issues** from the menu. The Issues window appears.
2. Click on the accounting process gap issue. The View Issue window appears.
3. Click **End Modification**. The issue is now closed.
4. Click **Send for Close Approval**. The issue is sent to the Issue Approver for closure.

Example: Issue Approver Reviews and Approves the Issue Closure

Gloria approves the issue closure. Complete these steps as Gloria:

1. Select **Issues and Action Plans > Issues** from the menu. The Issues window appears.
2. Click on the accounting process gap issue. The View Issue window appears.
3. Review the details of the issue. Gloria accepts the issue as closed. Click **Close Approved**, enter a **Change Reason**, and then click **Save**. The issue is now closed.

Chapter 9

Implementing Key Risk Indicators (KRIs) and KRI Workflows

Overview	97
KRIs and KRI Workflows	98
Overview	98
Roles for KRIs	99
KRI Process	100
Implementing Example KRIs	100
Example KRI Process	100
Example: Administrator Creates the KRI Validation Workflow	102
Example: Administrator Creates the KRI Definition for Number of Failed Trades	102
Example: Administrator Creates KRI Definition for Securities Department Headcount Growth	103
Example: Administrator Creates KRIs from the KRI Definitions	104
Example: Business Owner Creates KRI Observation Requests	105
Example: KRI Owner Provides KRI Scores	105
Example: KRI Validator Reviews KRI Scores	105
Example: Business Owner Submits Scores to Management Team	106
KRI Scoring	106
Overview	106
Calculating Lower, Upper, and Target Values When Values Are Unspecified	106
Normalization Method for Scale Types with Three Ranges	107
Normalization Method for Scale Type 4	108

Overview

Effective organizations use quantifiable metrics to assess performance and make strategic decisions as part of an effort to continually improve current and future operations. These metrics are called key performance indicators, or KPIs. Risk managers use a similar set of metrics to quantify and organize data related to risks and controls. These metrics are called key risk indicators, or KRIs. Just as KPIs can help organizations evaluate their success as it relates to long-term organizational goals, KRIs help risk managers determine the risk level of an organization. KRIs can give risk managers insight into strategically developing controls and processes to mitigate risks.

An example of a KRI would be the number of failed trades. In securities, a failed trade is one that does not settle on time. Failed trades can expose a securities trading desk to losses. For example, this can occur if the price of a security changes before the trade is settled. Therefore, a risk management team would want to track the number of failed

trades. An increase in the number of failed trades over time might indicate an execution problem within the company, or it could be symptomatic of wider, systemic market problems.

Key risk indicators are quantitative and can be currencies or percentages as well as other values. KRIs have a minimum and maximum value, as well as thresholds that indicate the normal operating range. Organizations typically modify these metrics over time to account for changes in the organization.

In some instances, KRIs are considered acceptable near or at the minimum or maximum value. For example, in the United States, a trading desk has had in the past three years a number of failed trades that range between 20 and 200 per month. An organization decides to set the minimum value to 0 (indicating no trades failed) and a maximum value of 400 (at which point the trading desk might stop trading to investigate). The organization sets the minimum threshold at 60 and the maximum threshold at 100. The minimum threshold is an indicator that the number of failed trades has reached a marginal range. Above the maximum threshold, the number of failed trades has reached an unacceptable range. If this occurs, the organization might decide to create an issue to investigate and mitigate the increased risk.

Other KRIs might be considered acceptable only if they lie between certain values. For example, the investment banking division might be hiring for a growing campus, and might set a headcount growth target of 15% for the year, to account for the overall growth of the trading desk. Growth less than 8% would indicate they are not hiring enough to meet their needs. But a growth target of 25% would indicate that they are overspending for the year. Growth between 10% and 20% would be considered acceptable.

Risk managers should first gather data about the type of measurement and the optimal ranges to use for their organizations before creating KRIs. For example, in the trading desk example, one trading desk might trade in much higher volumes than another. Therefore, the number of failed trades might be indicative of transactional volume rather than an internal or systemic problem. In this example, volume might also be indicative of organizational growth or changes in market volatility. Risk managers or other departmental experts should account for all of these factors.

This chapter uses the example of Orion Star, a bank that is using SAS Enterprise GRC to manage its GRC activities. Orion Star wants to use KRIs to monitor its securities transactions for risks in its trading operations, and to account for changes to their physical security department. The example uses the default SAS Enterprise GRC user interface environment. It assumes that you have completed the steps in previous chapters to create issues and action plans, assign users to the appropriate roles, and so on. It also assumes you understand the workflows for key risk indicators for this example. For more information about this example, see [Chapter 3, “Gathering Governance, Risk, and Compliance Data,”](#) on page 27.

Note: Your user interface might vary depending on the level of customization.

KRIs and KRI Workflows

Overview

SAS Enterprise GRC enables the process of managing KRIs and KRI workflows through the **KRI** menu. This menu enables you to perform the following tasks:

- Manage KRI definitions through the **Definitions** submenu. A KRI definition defines the risk area, ownership, and contains information about the type of KRI being measured. A KRI definition determines the default settings for corresponding indicators.

You must have assigned the KRI Definition capability to manage the **Definitions** submenu.

- Manage key risk indicators through the **Indicators** submenu. A KRI definition is used to create an indicator. The indicator specifies fields such as the owner, operational area, and threshold values.

You must have assigned the Indicator capability to manage the **Indicators** submenu.

- Manage requests through the **Requests** submenu. An indicator is used to create a request. A request asks the indicator owner for the level or value of the indicator at the defined time period. The request specifies fields such as the reporting period and the due date. After the request is created, it is sent to the owner of the corresponding indicator.

You must have KRI Observation or KRI Observation Request capabilities to manage the **Requests** submenu.

- Manage KRI workflows through the **KRI Validation Workflow** submenu. A KRI workflow specifies the validation stages (for a specific operational area) that are needed to complete a KRI request and observation process. Validation occurs according to the defined validation workflow.

You must have assigned the Validation Workflow capability to manage the **KRI Validation Workflow** submenu.

Roles for KRIs

Capabilities to manage KRIs are assigned through roles. The following table describes each role as it pertains to KRIs.

Table 9.1 Roles for KRIs

Role	Description
Enterprise GRC: Administration	Administrator. Administers the SAS Enterprise GRC environment. Might have responsibilities for maintaining KRI validation workflows and creating initial KRI definitions and KRIs.
Enterprise GRC: Business Ownership	Business Owner. Responsible for creating and maintaining KRIs, and creating KRI observation requests.
KRI Owner	Responsible for owning KRIs. Although there is no default SAS Enterprise GRC role for this person, a KRI Owner must have the View and Update capabilities for KRI observations, and the View capability for KRIs. KRI ownership can be performed by a number of SAS Enterprise GRC roles.

Role	Description
KRI Validator	Responsible for validating KRI observations. Although there is no default SAS Enterprise GRC role for this person, a KRI Validator must have the View capability for KRI observations and KRIs. KRI validation can be performed by a number of SAS Enterprise GRC roles.

Note: Depending on the capabilities of your assigned role, certain objects and fields in the user interface might be disabled for you during the completion of a task.

A single user could perform the tasks of all four roles. It is also possible for each role to be performed by a different user.

KRI Process

The KRI process is completed using the following steps:

1. The Administrator and Business Owner define and create the KRI definition, indicator, and workflow.
2. The Business Owner creates an observation request.
3. The KRI Owner provides a KRI observation score.
4. One or more KRI Validators review the KRI score and accept or reject the score. When the KRI has completed the validation process, the KRI validation state is now Fully Validated.
5. The Business Owner reviews the KRI score, and takes any necessary actions.

Implementing Example KRIs

Example KRI Process

Orion Star plans to track the number of failed trades in the Securities Department of its Investment Banking division, for their United States location. The organization wants to do this for each month. The unit of this measurement is a number. Values between 0 and 60 are considered acceptable. Values between 60 and 100 are considered medium. Values greater than 100 are considered high.

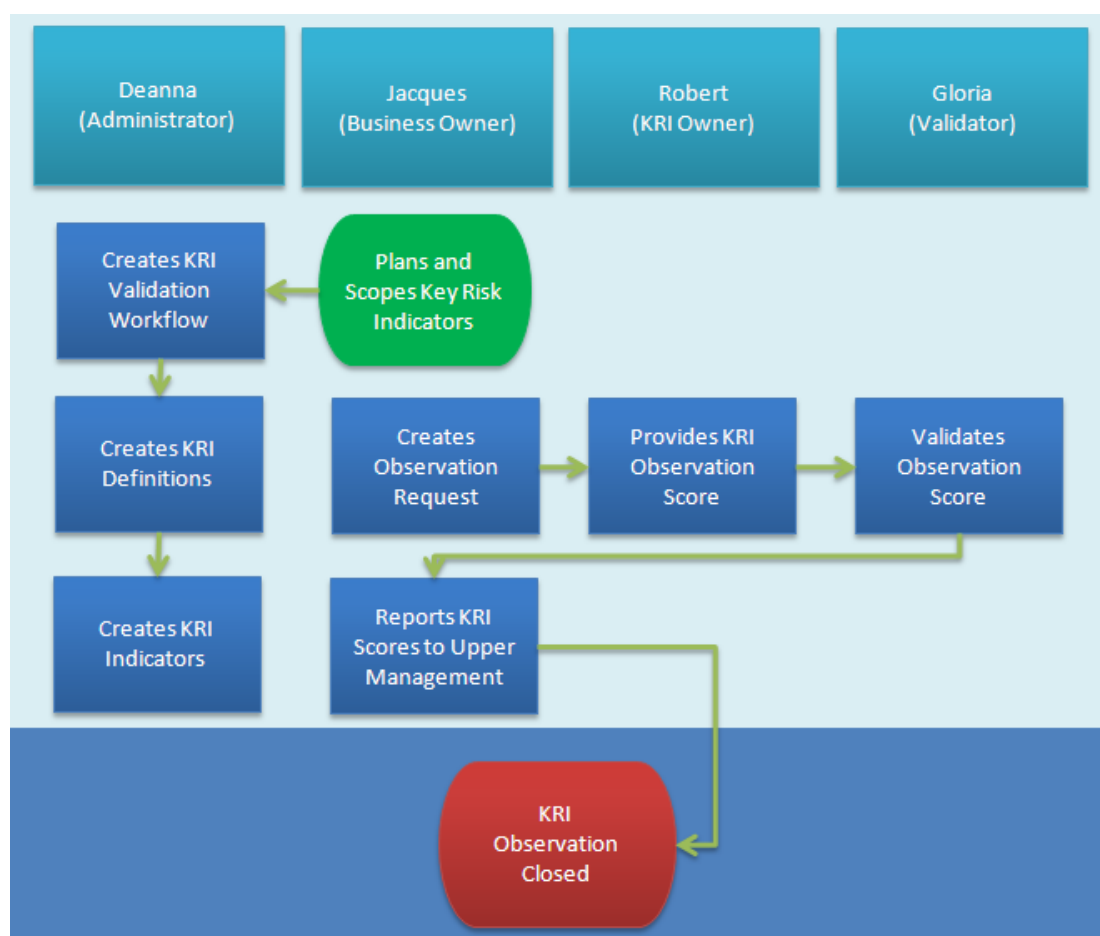
Orion Star also wants to track the growth of its Securities Department, specifically headcount for personnel, which has been targeted for 15% growth annually. The unit of this measurement is a percentage. Values between 0% and 8% are considered unacceptable. Values between 8% and 10% are considered marginal. Values between 10% and 20% are considered acceptable. Values between 20% and 25% are considered marginal. Values over 25% are considered unacceptable.

For the purpose of this example, the following table displays the users involved in controls and testing and their job titles and roles. The responsibilities and roles that you define vary depending on your organization.

Table 9.2 Example KRI Users and Roles

User	Job Title	SAS Enterprise GRC Roles
Deanna Tiswell	Administrator	Enterprise GRC: Administration
Jacques Simon	Central Operational Risk Manager, Investment Banking	Enterprise GRC: Business Ownership
Robert Fitzgerald	Securities Department Risk Manager	KRI Owner
Gloria Hyatt	Investment Banking Division Expert	KRI Validator

The following diagram illustrates the KRI process at Orion Star.

Display 9.1 KRI Process at Orion Star

The example below assumes that the business owner has already planned and scoped key risk indicators for the Securities Department, and passed this information to Deanna, the administrator.

The example follows these steps:

1. Deanna, the Administrator, [creates the KRI validation workflow](#).
2. Deanna [creates a KRI definition](#) for the failed trades KRI.
3. Deanna [creates a KRI definition](#) for the headcount growth KRI.
4. Deanna [creates KRIs](#) using the KRI definitions as templates.
5. Jacques, the Business Owner, [creates KRI observation requests](#).
6. Robert, the KRI Owner, [provides a KRI score for each request](#).
7. Gloria, the KRI Validator, [reviews and validates the KRI scores](#).
8. Jacques [reviews and submits the KRI scores](#).

Example: Administrator Creates the KRI Validation Workflow

Deanna creates the KRI validation workflow as Administrator. Complete these steps as Deanna:

1. Select **KRI > KRI Validation Workflow** from the menu. The KRI Validation Workflow window appears.
2. Select the operational area for the issue. In the OL chooser, click **Edit** and in the Operational Point window, select the following dimensions and nodes from the **Dimension** drop-down list and click **Add** for each.
 - Dimension: **Management Organization**
Node: **Management Organizations > iFinance > Investment Banking > Securities**
 - Dimension: **Geography**
Node: **Geographies > Americas > North America > United States**

Click **OK** to add the operational point and return to the previous window.
3. In the Current Validation Stages table, click **Create Validation Stages**. The Edit Validation Stages window appears.
4. Click **Add Validation Stage**. The Add Validation Stage window appears.
5. Enter the name of the validation stage, *Validation Stage for Securities Department*, in the **Name** field.
6. In the Validators table, click **Add User**. The View Users window appears. Select **Gloria** as the Validator and return to the Add Validation Stage window.
7. Click **OK** to return to the Edit Validation Stages window.
8. This validation does not require multiple validation stages. Click **Save**, enter a reason for the change in the Change Reason window, and click **Save** again.

Example: Administrator Creates the KRI Definition for Number of Failed Trades

Deanna creates a KRI definition for the failed trades indicator as Administrator. Complete these steps as Deanna:

1. Select **KRI > Definitions** from the menu. The Definitions window appears.

2. Click **Create Definition**. The Create KRI Definition window opens
3. Select the operational area for the issue. In the OL chooser, click **Edit**. In the Operational Point window, select the following dimensions and nodes from the **Dimension** drop-down list and click **Add** for each.
 - Dimension: **Management Organization**
Node: **Management Organizations > iFinance > Investment Banking > Securities**
 - Dimension: **Geography**
Node: **Geographies > Americas > North America > United States**

Click **OK** to add the operational point and return to the previous window.
4. On the Details tab, enter the name of the definition, *Failed Trades*. Keep all other defaults and click the **Owner** tab.
5. On the Owner tab, accept the default (no owner) and click the **Measurement** tab.
6. On the Measurement tab, enter measurement information. Complete these steps:
 - a. Select **Number** in the **Unit of Measure** field.
 - b. The number of failed trades is tracked on a monthly basis. Select **Monthly** in the **Interval** field.
 - c. The scale for the indicator is a minimum maximum scale type with three ranges. Select **Scale (3)** in the **Scale Type** field.
Note: This option appears only if you have configured functionality for certain scale types that are not included by default in SAS Enterprise GRC by default. For more information about enabling scale types for this example, see the *SAS Enterprise GRC: Administration and Customization Guide*.
 - d. The number of failed trades is a predictive indicator of increased risk. Select **Predictive** in the **KRI Nature** field.
 - e. The number of failed trades is a risk frequency indicator. Select **Risk Frequency** in the **KRI Type** field.
 - f. Click the **Thresholds** tab.
7. On the Thresholds tab, enter the KRI thresholds. Complete these steps:
 - a. Enter *0* in the **Minimum Value** field.
 - b. Enter *60* in the **Lower Threshold Value** field.
 - c. Enter *100* in the **Upper Threshold Value** field.
 - d. Enter *200* in the **Maximum Value** field.
 - e. Select **As the values decrease, the indicator is improving** in the **Interpretation** field.
8. Click **Save** to save the definition.

Example: Administrator Creates KRI Definition for Securities Department Headcount Growth

Deanna creates a KRI definition for the headcount growth indicator as Administrator. Complete these steps as Deanna:



1. Select **KRI > Definitions** from the menu. The Definitions window appears.
2. Click **Create Definition**. The Create Definitions window opens
3. Select the operational area for the issue. In the OL chooser, click **Edit**. In the Operational Point window, select the following dimensions and nodes from the **Dimension** drop-down list and click **Add** for each.
 - Dimension: **Management Organization**
Node: **Management Organizations > iFinance > Investment Banking > Securities**
 - Dimension: **Geography**
Node: **Geographies > Americas > North America > United States**

Click **OK** to add the operational point and return to the previous window.
4. On the Details tab, enter the name of the definition, *Securities Department Headcount Growth*. Keep all other defaults and click the **Owner** tab.
5. On the Owner tab, accept the default (no owner) and click the **Measurement** tab.
6. On the Measurement tab, enter measurement information. Complete these steps:
 - a. Select **Number** in the **Unit of Measure** field.
 - b. Headcount growth is tracked on an annual basis. Select **Annually** in the **Interval** field.
 - c. Headcount growth is a predictive indicator of increased risk. Select **Predictive** in the **KRI Nature** field.
 - d. Headcount growth is a risk exposure indicator. Select **Risk Frequency** in the **KRI Type** field.
 - e. The scale for the indicator is a central scale type with four ranges. Select **Scale (4)** in the **Scale Type** field.
 - f. Click the **Thresholds** tab.
7. On the Thresholds tab, enter the KRI thresholds. Complete these steps:
 - a. Enter 8 in the **Minimum Value** field.
 - b. Enter 10 in the **Lower Threshold Value** field.
 - c. Enter 15 in the **Target Value** field.
 - d. Enter 20 in the **Upper Threshold Value** field.
 - e. Enter 200 in the **Maximum Value** field.
 - f. Select **As the values move toward the target from either direction, the indicator is improving** in the **Interpretation** field.
8. Click **Save** to save the KRI definition.

Example: Administrator Creates KRIs from the KRI Definitions

Deanna, the Administrator, creates KRIs using the KRI definitions as a template. For each KRI definition that you have created, complete these steps as Deanna:


1. Select **KRI > Definitions** from the menu. The Definitions window appears.

2. Click the Create Indicator icon  next to the KRI definition that you created in the previous task. The Create Indicator window appears.
3. Click the **Owner** tab.
4. On the **Owner** tab, click the Select User icon  to select the **Owner** of the Indicator. The View Users window appears. Select **Robert** as the KRI Owner. Click the **Thresholds** tab.
5. On the Thresholds tab, select **Yes** in the **Allow Values Outside the Defined Range** field.
6. Click **Save** to save the KRI.

When you have created both indicators, log off from SAS Enterprise GRC.

Example: Business Owner Creates KRI Observation Requests

At the end of the month, Jacques, the Business Owner, creates KRI observation requests for both KRIs that Deanna has created. For each indicator, complete these steps as Jacques:

1. Select **KRI > Indicators** from the menu. The Indicators window appears.
2. For the appropriate indicator, click the Create Request icon . The Create Request window appears.
3. Select an appropriate date in the **Due Date** field. Accept the other defaults, review the response scale, and click **Save**.

When you have created both requests, log off from SAS Enterprise GRC.

Example: KRI Owner Provides KRI Scores

Robert, the KRI owner, provides a KRI score for each request and sends the KRI scores for validation. Complete these steps as Robert:

1. Robert has received notification via the task list that he needs to submit the indicator for the number of failed trades. Click on the task link. The observation window appears for the task.
2. Robert has observed that there were 75 failed trades in the past month. Enter 75 in the **Score** field, and accept the other defaults. Click **Send for Validation**.
3. Robert has also received notification via the task list that he needs to submit the indicator for the headcount growth. Click on the task link. The observation window appears for the task.
4. Robert has also observed that the growth rate has been 9% the past year. Enter 7 in the **Score** field, and accept the other defaults. Click **Send for Validation**.
5. Log off from SAS Enterprise GRC.

Example: KRI Validator Reviews KRI Scores

Gloria, the KRI validator, reviews the KRI scores and confirms the KRI scores are accurate as provided.

Complete these steps as Gloria:

1. Gloria has received notification via the task list that she needs to validate the failed trades indicator. For more information about KRI score normalization, see “[KRI Scoring](#)” on page 106.

Gloria is satisfied with the KRI score as observed. Click on the task link. On the indicator window, review the indicator, and click **Validate**. The KRI is now fully validated.

2. Repeat the preceding step to validate the headcount growth indicator.
3. Log off from SAS Enterprise GRC.

Example: Business Owner Submits Scores to Management Team

Jacques then submits the KRI score to the management team. If either KRI score has exceeded a threshold level, Jacques might need to investigate or create a corresponding issue and take action. In this case, the problem is marginal for both observations and Jacques intends to closely monitor the item, but does not take any actions at this time.

KRI Scoring

Overview

When a score is submitted by an owner for validation, SAS Enterprise GRC calculates a normalized score. This normalized score enables a validator to compare scores that have different threshold values and different interpretations.

There are two types of normalization methods, depending on the scale type. A scale type of 3 pertains to a scale with three ranges, whereas a scale type of 4 pertains to a scale with 5 ranges.

For both normalization methods, the following values are defined as follows:

- s score provided by the owner
- m minimum value of measurement
- l lower threshold value of measurement
- u upper threshold value of measurement
- M maximum value of measurement
- t target value of measurement (only used for five range scale normalization methods)
- z normalized score

Calculating Lower, Upper, and Target Values When Values Are Unspecified

When you specify values for an indicator, you must specify values for minimum and maximum values. However, you can choose not to provide values for the lower threshold, upper threshold, and target. (Target values only apply to Scale Type 4 indicators.) If you do not provide these values, the solution automatically calculates these values using the following formulas.

For lower threshold values, the value is calculated as follows:

$$l = m + \frac{M - m}{3}$$

For upper threshold values, the value is calculated as follows:

$$u = m + \frac{2(M - m)}{3}$$

For target values in a scale type 4 approach, the value is generally calculated as follows:

$$t = \frac{l + u}{2}$$

Certain caveats apply. For the scale type 4 approach, if you provide a minimum, maximum, and target but not lower or upper threshold values, the lower and upper threshold values are adjusted: If the lower threshold is greater than the target, the lower threshold is equal to the target value. If the upper threshold is less than the target, the upper threshold is equal to the target. For either approach, if either one of the lower or upper threshold values are left missing, you must fill in the missing value for the other threshold. (For example, if you specify an upper threshold, you must supply a lower threshold value also.)

When you save the KRI, in cases where values were left unspecified, a message will appear that provides the new values as calculated by the solution.

Note: The number of trailing digits used in the calculation is determined by the `monitor.kri.maxFractionDigits` property (the default is 2).

Normalization Method for Scale Types with Three Ranges

For scales with three range values, the following normalization methods apply.

If increasing values of the indicator are favorable, then the normalized score is calculated using the following formula:

$$z = \begin{cases} \frac{s-m}{3(\ell-m)} & \text{if } s \leq \ell \\ \frac{1}{3} + \frac{s-\ell}{3(u-\ell)} & \text{if } \ell < s \leq u \\ \frac{2}{3} + \frac{s-u}{3(M-u)} & \text{if } s > u \end{cases}$$

If increasing values of the indicator are not favorable, then the normalized score equals one minus the result of the above formula. If the score provided by the owner is within the defined range, then the normalized score is between zero and one.

There are a number of alternative methods that can be used to calculate the normalized KRI observation value. The method used depends on the scale. Again, normalized values are from 0 to 1. Here are examples that show the methods for calculating these values:

- The observation **s** is on a scale from 0 to a maximum **M**. For example, on a scale from 0 to 100, an **s** value of 65 is normalized to .65 (that is, the observation value 65 is divided by the high limit 100).
- The observation **s** is on a scale from a minimum (**m**) to a maximum (**M**). The normalized value is $(s - m) / (M - m)$. For example, on a scale from 20 to 40, a KRI

observation of 30 becomes $(30 - 20)/(40 - 20) = 10/20$. Hence, 30 becomes normalized to 0.5.

- The score is normalized as one of the set including the lower threshold (**l**) and the upper threshold (**u**). The set is then (**m**, **l**, **u**, **M**).

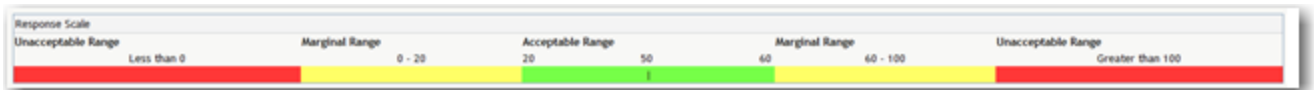
For example, assume that there is a color scale where red is bad, yellow is okay, and green is good. Imagine applying this scale to test scores, where 0 to 60 is bad (red), 60 to 80 is okay (yellow), and 80 to 100 is good (green). Each color is provided 1/3 of the total. This means the following:

- A score of 0 is the lowest possible (normalized to 0).
- A score of 100 is the highest possible (normalized to 1).
- A score of 60 is the high end of the lowest scale (normalized to 1/3).
- A score of 80 is the high end of the middle scale (normalized to 2/3).
- A score of 70 would be half way between 1/3 and 2/3 (normalized to $1/2 = .5$).
- A score of 90 would be half way between 2/3 and 1 (normalized to 5/6).

When scores are normalized, it is important to note how these calculations are rounded. For example, assume that you have a range with the following thresholds: $m = 0$, $l = 20$, $u = 40$, and $M = 80$. If your score is 41, your normalized value should be $2/3 + (41-40)/3(80-40) = 0.675$. In this instance, the value of 2/3 is rounded to 0.6666666666666667 instead of 0.6666666666666666. This is because if the latter value were used, the value would be 0.6749999999999999. Therefore, when the final value is finally rounded to the specified trailing digits, by default this normalized value would be rounded down to 0.67 and not up to 0.68.

Normalization Method for Scale Type 4

Scales with five ranges are displayed as follows:



The formulas that are used apply normalization methods that are similar to the three range scale.

For values that are targeted outside the scale range, the following formulas are used:

- If the score is less than the minimum value, then this formula is used:

$$z = \frac{2}{3} - \left(\frac{s - m}{3(l - m)} \right)$$

- If the score is less than the lower threshold but greater than the minimum, then this formula is used:

$$z = \frac{1}{3} + \left(\frac{l - s}{3(l - m)} \right)$$

- If the score is less than the target but greater than the lower threshold, then this formula is used:

$$z = \frac{(t - s)}{3(t - l)}$$

- If the score is greater than or equal to the target but less than the upper threshold, then this formula is used:

$$Z = \frac{(s - t)}{3(u - t)}$$

- If the score is greater than the upper threshold but less than the maximum, then this formula is used:

$$Z = \frac{1}{3} + \left(\frac{s - u}{3(M - u)} \right)$$

- If the score is greater than the maximum value, then this formula is used:

$$Z = \frac{2}{3} + \left(\frac{s - M}{M - u} \right)$$

For values that are centered to an in-between target value, the following formulas are used:

- If the score is less than the minimum value, then this formula is used:

$$Z = \frac{1}{3} - \left(\frac{m - s}{3(l - m)} \right)$$

- If the score is less than the lower threshold but greater than the minimum, then this formula is used:

$$Z = \frac{1}{3} + \left(\frac{s - m}{3(l - m)} \right)$$

- If the score is less than or equal to the target but greater than the lower threshold, then this formula is used:

$$Z = \frac{2}{3} + \left(\frac{s - l}{3(t - l)} \right)$$

- If the score is greater than the target but less than the upper threshold, then this formula is used:

$$Z = \frac{2}{3} + \left(\frac{u - s}{3(u - t)} \right)$$

- If the score is greater than the upper threshold but less than the maximum, then this formula is used:

$$Z = \frac{1}{3} + \left(\frac{M - s}{3(M - u)} \right)$$

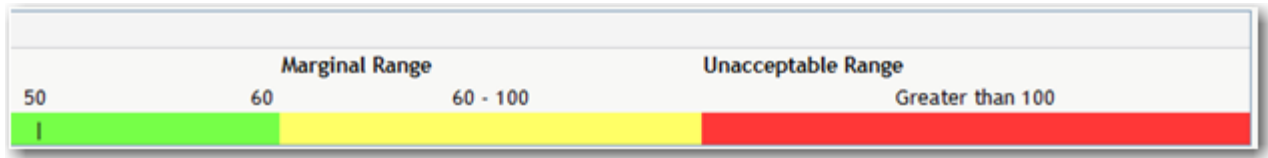
- If the score is greater than the maximum value, then this formula is used:

$$Z = \frac{1}{3} - \left(\frac{(s - M)}{3(M - u)} \right)$$

When scores are normalized, it is important to note how these calculations are rounded. For example, assume that you have a range with the following thresholds: $m = 5000$, $l = 30000$, $u = 100000$, and $M = 200000$. If your score is 4375, your normalized value should be $2/3 - (4375 - 5000)/3(30000 - 5000) = 0.675$. In this instance, the value of $2/3$ is rounded to 0.6666666666666667 instead of 0.6666666666666666. This is because if the latter value were used, the value would be 0.6749999999999999. Therefore, when the final value is finally rounded to the specified trailing digits, by default this normalized value would be rounded down to 0.67 and not up to 0.68.

Because the normalized score is a derivative of a percentage value for a given range size, the score cannot be predicted outside of these values. This is because the percentage cannot be calculated. SAS Enterprise GRC uses a normalization approach that addresses values outside of the minimum and maximum range by projecting the threshold for the minimum or maximum range values onto the outside ranges.

For example, assume that the preceding scale is used. The following figure shows the right side of this scale.

Display 9.2 Dividing the Five Range Scale

This example, which uses a centered scale, has an upper threshold of 60 and a maximum value of 100. This indicates that the marginal range size is 40 (100-60). This range size is then used to calculate where a normalized score falls relative to values greater than 100.

The value for a reported score of 140 is therefore $z = \frac{1}{3} - \left(\frac{(s - M)}{3(M - u)} \right)$, for a centered scale, which is then calculated as follows:

$$z = \frac{1}{3} - \left(\frac{140 - 100}{3(100 - 60)} \right) = 0.0$$

Chapter 10

Implementing Controls and Control Tests

Overview	111
Controls and Control Testing Workflows	112
Overview	112
Control and Control Testing Definitions	112
Roles for Control Testing	113
Control Testing and Test Approval Process	114
Implementing an Example Control Test	115
Example Control Testing Process	115
Defining Control Testing Data Objects	117
Example: Control Owner Creates Control	117
Example: Central Risk Manager Approves the Control	118
Example: Test Coordinator Creates the Test Definition	118
Example: Test Definition Approver Reviews and Approves the Test Definition ..	119
Example: Test Owner Creates a Test	119
Example: Tester Accepts Test, Completes Test, and Submits Results	120
Example: Test Results Approver Reviews and Approves the Test Results	120
Example: Control Owner Reviews and Approves the Control	121
Example: Control Certification Owner Reviews and Certifies the Control	121

Overview

In risk management, *controls* are used to mitigate or reduce risks. For example, in an IT environment, an organization could be exposed to IT security threats that could cause system outages, expose data to loss or leakage of information, or damage physical assets. To mitigate these risks, IT organizations implement software and hardware controls (for example, anti-virus software, firewalls, or data center redundancies).

To ensure that these controls are functioning properly, organizations that implement GRC use a control testing workflow process to periodically review controls for adequacy and effectiveness, and to certify the controls. The control testing workflow enables accountability and creates a traceable information stream for reporting purposes. Periodic control testing has become common practice among large companies with the introduction of the Sarbanes-Oxley Act of 2002. This law requires that stock-listed public companies or their parent organizations perform control effectiveness tests on at least an annual basis, the results of which then need to be certified by an external auditor.

This chapter uses the example of Orion Star, a bank that is using SAS Enterprise GRC to manage its GRC activities. The example uses the default SAS Enterprise GRC user

interface environment, and assumes that data has already been gathered about controls and control test workflows, users have been assigned to the appropriate roles, and that controls and control tests are either developed or are in development. For more information about this example, see [Chapter 3, “Gathering Governance, Risk, and Compliance Data,” on page 27](#).

Note: Your user interface might vary depending on the level of customization.

Controls and Control Testing Workflows

Overview

SAS Enterprise GRC enables the process of creating controls and developing control tests and workflows through the **Control Testing** menu. This menu enables you to perform the following tasks:

- Manage controls through the **Controls** submenu. A control is an action taken to manage a risk.

You must have Control capabilities to manage the **Control** submenu.

- Manage test definitions and tests through the **Test Definitions** and **Tests** submenus. Tests are mechanisms to assess controls for a specific time period. A test contains exactly one control. A test definition is a template used for creating tests, and can contain multiple controls.

You must have Test Definition capabilities to manage the **Test Definitions** submenu.

- Manage test definition groups through the **Test Definition Groups** submenu. A test definition group contains several test definitions. For more information about control testing measures, see [“Control and Control Testing Definitions” on page 112](#).

You must have **Test Definition Group** capabilities to view the **Test Definition Groups** submenu.

- Manage control testing measures, test periods, certification periods, and business policies through the **Libraries** submenu. For more information about these items, see [“Control and Control Testing Definitions” on page 112](#).

The **Libraries** submenu is always available when users have the capability to access the **Control Testing** menu.

Control and Control Testing Definitions

The following definitions apply to the control and control testing process:

certification

an evaluation of a control for a control testing measure during a specific time period.

certification period

period of time for which a control is certified. A control can be certified only once per certification period. It is possible to have multiple certification periods that cover the same calendar period, with each certification period having a different control testing measure.

control testing measures

a measure used to evaluate an attribute of a control. Examples of control attributes are adequacy and effectiveness. Adequacy measures how well a control is documented and whether the control is being executed in a way that the control conduct owner expects. Effectiveness measures how well a control mitigates the corresponding risks. For example, suppose a control is in place that prevents employees from working overtime. The purpose of the control is to keep employees from being dissatisfied with their employment and leaving your organization. Suppose now that employees are no longer working overtime, but the employee turnover rate has not changed. This example demonstrates an adequate, but ineffective, control.

control testing responses

a list of possible values for a control testing measure. A control testing measure always has exactly one response scale, but that scale can consist of any number of responses. For example, a response scale could include the following two responses: inadequate and adequate.

test period

period of time for which a control is tested. A control can be tested only once per test period. Exactly one control testing measure is specified for each test period. It is possible to have multiple test periods that cover the same calendar period, with each test period having a different control testing measure.

Roles for Control Testing

Capabilities to test controls are assigned through roles. The following table describes each role as it pertains to control testing.

Table 10.1 *Roles for Control Testing*

Role	Description
Enterprise GRC: Administration	Administrator. Administers the SAS Enterprise GRC environment. Might have responsibilities for maintaining control testing workflows.
Enterprise GRC: Control Ownership	Control Owner. Responsible for the creation, ownership, and administration of controls, and approving control test results.
Enterprise GRC: Control Certification Ownership	Control Certification Owner. Responsible for certifying test results.
Enterprise GRC: Test Coordination	Test Coordinator. Responsible for creating and managing control test definitions and control tests.
Enterprise GRC: Test Definition Approval	Tester Definition Approver. Responsible for reviewing and approving test definitions.
Enterprise GRC: Test Ownership	Test Owner. Person responsible for the testing process.
Enterprise GRC: Testing	Tester. Responsible for performing control tests.

Role	Description
Enterprise GRC: Test Results Approval	Test Results Approver. Person responsible for reviewing and approving test results.

Note: Depending on the capabilities of your assigned role, certain objects and fields in the user interface might be disabled for you during the completion of a task.

Control Testing and Test Approval Process

The control testing process is completed using the following steps:

1. The Administrator works with the Risk Manager, Control Owner, Test Coordinator, and Test Owner to initially define the following in SAS Enterprise GRC:
 - controls
 - control test workflows
 - control test periods
 - control certification periods
 - control testing measures
 - control testing responses
 - test definitions and test definition groups
 - control tests

Responsibilities are also assigned to any users during this step.

2. The Control Owner creates a new control. The person assigns a Control Owner and a Control Certification Owner to the control.
3. The Test Coordinator works with the Test Owner and Testers to gather data about tests and creates the template for the tests, called a test definition. The Test Coordinator selects the controls to add to the test definition. Although the test definition can contain multiple controls, each test created from the test definition has only one control. The Test Coordinator also assigns a Test Owner to each test definition, and can assign Testers as needed. The Test Coordinator sends the test definition for approval.
4. Test Definition Approvers review the information and approve the test definition. The test definition is now fully approved.
5. The Test Owner plans and creates a test from an approved test definition. The Test Owner selects which control to test, assigns Testers to complete the test, and then publishes the test.
6. Testers accept the test and execute the test according to the testing plan. After the test has been executed, Testers report on various measures, such as the effectiveness or adequacy of the control. The test is then sent for approval.
7. Test Results Approvers review the information and approve the test results.
8. The Control Owner reviews and approves the test results. The test is now fully approved.
9. Control Certification Owners review the fully approved test and create a control certification for the control. The control is now certified.

Implementing an Example Control Test

Example Control Testing Process

The securities department at Orion Star is rolling out their risk management infrastructure, and is implementing controls to mitigate risks. These controls also require a control testing and certification process to monitor these controls and ensure their proper functioning. For the purpose of this example, the following table displays the users involved in controls and testing and their job titles and roles. The responsibilities and roles that you define vary depending on your organization.

Table 10.2 Example Control Testing Users and Roles

User	Job Title	SAS Enterprise GRC Roles
Deanna Tiswell	Administrator	Enterprise GRC: Administration
Robert Fitzgerald	Securities Department Risk Manager	Enterprise GRC: Control Ownership Enterprise GRC: Local Risk Management
Jacques Simon	Central Operational Risk Manager, Investment Banking	Enterprise GRC: Central Risk Management
Samantha Glass	Risk Coordinator	Enterprise GRC: Test Coordination Enterprise GRC: Test Ownership
Mike Hume	IT Security Analyst	Enterprise GRC: Testing
Gloria Hyatt	Investment Banking Division Expert	Enterprise GRC: Test Definition Approval Enterprise GRC: Test Results Approval
Wendy Feinstein	Securities Department Investigator	Enterprise GRC: Control Certification Ownership

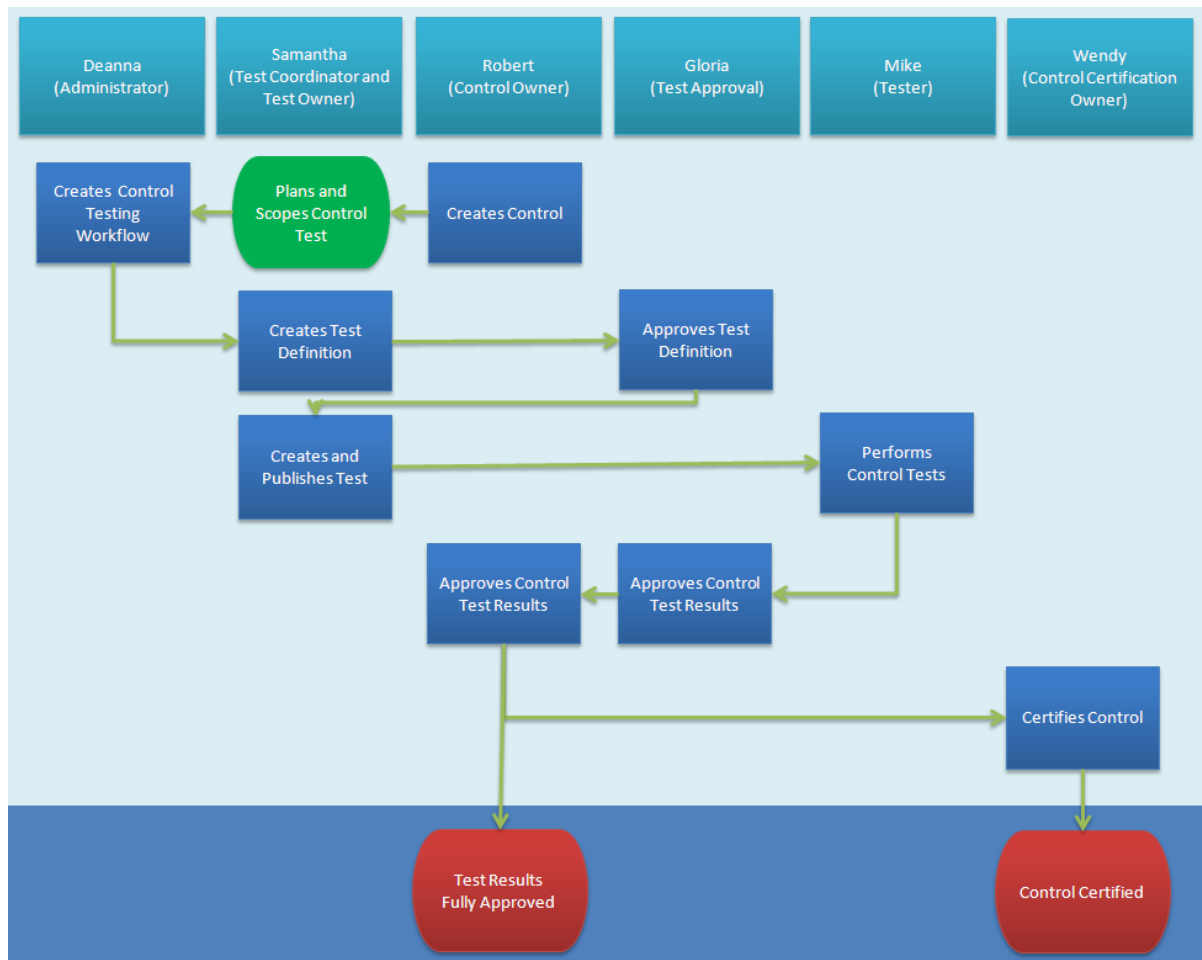
In this example, the IT Security group at Orion Star is installing a network firewall device to keep intruders from attacking open network ports and compromising data within its environment, as part of its overall IT security strategy. This firewall control is redundant, so that when one firewall device goes down, a second firewall is made available, and business can occur normally without interruption or security compromise. These devices are assets under the purview of the Securities Department. Therefore, Robert is the control owner.

The Risk Coordinator, Samantha, plans to test this control on a quarterly basis by directing its IT Security Analyst, Mike, to perform a series of steps to check the device for business continuity problems. These tests are approved by Gloria. The control is also certified on a quarterly basis by the Securities Department Investigator, Wendy, to ensure it is working effectively to reduce the risk of intrusion and data compromise or loss.

This example assumes that you are using the sample data, and that the following library objects have already been created: control testing measures, test periods, and certification periods.

The following figure describes this process for the example of Orion Star.

Display 10.1 Example Control Testing Workflow



The example follows these steps:

1. Robert, as Control Owner and Local Risk Manager, creates the control, assumes ownership, assigns Wendy as the Control Certification Owner, and approves the control.
2. Jacques, as Central Risk Manager, approves the control.
3. Samantha, as Test Coordinator, creates the test definition.
4. Gloria, as Test Definition Approver, approves the test definition.
5. Samantha, as Test Owner, creates and publishes the test.

6. Mike, as Tester, [accepts the test, tests the control, and submits the results.](#)
7. Gloria, the Test Results Approver, [approves the test results.](#)
8. Robert, the Control Owner, [approves the test results.](#)
9. Wendy, the Control Certification Owner, [certifies the control.](#)

Defining Control Testing Data Objects

Before initiating a control testing process, you must define several data objects to be used in the process. You can define some of these objects outside of SAS Enterprise GRC and then data load them into the application. You can create others directly in the user interface.

These data objects can be viewed and managed on the **Libraries** submenu that you access from the **Control Testing** menu.

The following data objects are used for the control testing process:


- control testing measures
- test periods
- certification periods
- business policies


For more information about the procedures to create, load, modify, and remove these objects, see the *SAS Enterprise GRC: Help*.

Example: Control Owner Creates Control

Robert creates a new control as Control Owner. Complete these steps as Robert:

1. Select **Control Testing > Controls** from the menu. The Controls window appears.
2. Click **Create** and select **Control**. The Create Control window appears.
3. Enter the details of the control. Complete these steps:
 - a. Select the operational area for the control. In the OL chooser, click **Edit** and in the Operational Area window, select the following dimensions and nodes from the Dimension drop-down list and click **Add** for each.
 - Dimension: **Management Organization**
Node: **Management Organizations > iFinance > Investment Banking > Securities**
 - Dimension: **Geography**
Node: **Geographies > Americas > North America > United States**

Click **OK** to add the operational area and return to the previous window.
 - b. Enter *Network Firewall* in the **Control Title** field.
 - c. Select **IT Systems > Review and update the systems security infrastructure** in the **Control Type** tree.
 - d. In the **Control Conduct Owner** field, click on the Select User icon (). If it is not already selected, select **Robert Fitzgerald** as the control owner.

- e. In the **Control Certification Owner** field, click on the Select User icon (). Select **Wendy Feinstein** as the control certification owner.
4. Accept the defaults for the remaining fields. Click **Apply** to save the control.
5. Because Robert is also the local risk manager, he can also send the control for approval. Click **Send for Approval** to send the control approval to the control owner.
6. Because Robert is also the control owner, he can approve the control. From the Controls window, click the control Click **Approve**, enter a **Change Reason**, and click **Save**. The control is sent to Jacques for approval.
7. Log off from SAS Enterprise GRC.

Example: Central Risk Manager Approves the Control

Jacques approves the control as Central Risk Manager. Complete these steps as Jacques:


1. Select **Control Testing > Controls** from the menu. The Controls window appears.
2. Click on the network firewall control. The View Control window appears.
3. Review the details of the control. Jacques is satisfied with the control information. Click **Approve**, enter a **Change Reason**, and click **Save**. The control is now fully approved.
4. Log off from SAS Enterprise GRC.

Example: Test Coordinator Creates the Test Definition

Samantha creates the test definition as Test Coordinator. Complete these steps as Samantha:

1. Select **Control Testing > Test Definitions** from the menu. The Test Definitions window appears.
2. Click **Create Test Definition**. The Create Test Definition window appears.
3. Select the operational area for the control. In the OL chooser, click **Edit** and in the Operational Area window, select the following dimensions and nodes from the Dimension drop-down list, and click **Add** for each.
 - Dimension: **Management Organization**
Node: **Management Organizations > iFinance > Investment Banking > Securities**
 - Dimension: **Geography**
Node: **Geographies > Americas > North America > United States**

Click **OK** to add the operational area and return to the previous window.
4. In the Controls table, click **Add Controls**. The Add Controls window appears.
Select the **IT Systems > Review and update the systems security infrastructure** check box. Click **Add and Close** to return to the Create Test Definition window.
5. Enter the test details. Complete these steps:
 - a. Enter *Network Firewall Test* in the **Test Definition Title** field.

- b. Samantha has dual roles, as both the Test Coordinator and Test Owner, in this example. In the **Test Owner** field, click on the Select User icon () and select **Samantha Glass** as the test owner.
- c. Select the dates for which the test definition is active. Provide an appropriate date in the **Active-From Date** and **Active-To Date** fields.
- d. Enter information about the **Testing Procedure**. For example, enter *Power off main network firewall device, see if secondary device takes over.*
You can also attach a file that provides the details of the testing procedure.
6. The test measures the effectiveness of the control. In the Measures table, click **Link Measures**. The Select Measure Entries to Link window appears.
Select **Effectiveness**, and click **Add and Close** to return to the Create Test Definition window.
7. Accept the other default, click **Apply**, and then click **Send for Approval**. The test definition is sent to the Test Definition Approver.
8. Log off from SAS Enterprise GRC.



Example: Test Definition Approver Reviews and Approves the Test Definition

Gloria approves the test definition as Test Definition Approver. Complete these steps as Gloria:

1. Select **Control Testing > Test Definitions** from the menu. The Test Definitions window appears.
2. Click on the network firewall test definition. The View Test Definition window appears.
3. Review the details of the test definition. Gloria is satisfied that the new test covers all criteria. Click **Approve**, enter a **Change Reason**, and click **Save**. The test definition is now fully approved.
4. Log off from SAS Enterprise GRC.

Example: Test Owner Creates a Test

Samantha creates the test. Complete these steps as Samantha:

1. Select **Control Testing > Test Definitions** from the menu. The Test Definitions window appears.
2. Click on the Create Tests icon () . The Create Tests from Test Definition window appears.
3. In the Tests table, click the Row Action icon () to access the action menu, and select **Manage Testers**. The Manage Testers for Control window appears.
4. **Users** is the option selected by default. Click **Add Users**. The Add Testers for Control window appears.
5. Select the check box next to **Mike Hume**, and click **Add and Close** to return to the Manage Testers for Control window. Then click **OK** to return to the Create Tests from Test Definition window.

6. Enter *Network Firewall Test* in the **Reference** field.
7. Select a test period from the **Test Period** drop-down list.
8. Select the due date for the test to be completed. Provide an appropriate date in the **Due Date** field.
9. Click **Publish** to send the test to the Tester, Mike for testing.
10. Log off from SAS Enterprise GRC.

Example: Tester Accepts Test, Completes Test, and Submits Results

Mike accepts the test, completes the test, and submits the results. Complete these steps as Mike:

1. Mike has received notification via the task list that he needs to accept the test. Click on the task link, and in the View Test window, review the test and click **Accept**. The Edit Test window appears, in the **Test Details** subtab.
2. Mike runs the test on the control, the network firewall device. When he boots the firewall device, the redundant firewall device works as it should. He does the same on the redundant device and it performs a fail-over correctly. He repeats this test five times, and it does not fail. In the **Test Results** area of the window, enter the following information:
 - **Test Sample Description:** Enter *Performed reboot cycle 5 times*.
 - **Sample Size:** Select **Number**.
 - **Actual Sample Size:** Enter *5*.
 - **Actual Sample Failed:** Enter *0*.
3. Click on the **Responses** subtab, and in the Responses area, select **Effective** as the response.
4. Accept the other defaults and click **Send for Approval**, enter a **Change Reason**, and click **Save**. The test results are sent to Gloria, the Test Results Approver.
5. Log off from SAS Enterprise GRC.

Example: Test Results Approver Reviews and Approves the Test Results

Gloria receives notification that the test results are submitted, and approves the test results. Complete these steps as Gloria:

1. Select **Control Testing > Tests** from the menu. The Tests window appears.
2. Click on the network firewall test. The View Test window appears.
3. Review the results of the test. Gloria is satisfied that the new test results are correct. Click **Approve**, enter a **Change Reason**, and click **Save**. The test is now sent to the Control Owner, Robert.
4. Log off from SAS Enterprise GRC.


Example: Control Owner Reviews and Approves the Control

Robert receives notification that the test results are submitted, and approves the test results. Complete these steps as Robert:

1. Select **Control Testing > Tests** from the menu. The Tests window appears.
2. Click on the network firewall test. The View Test window appears.
3. Review the results of the test. Robert is satisfied that the new test results are correct. Click **Approve**, enter a **Change Reason**, and click **Save**. The test is now Fully Approved.
4. Log off from SAS Enterprise GRC.

Example: Control Certification Owner Reviews and Certifies the Control

Wendy, the Control Certification Owner, reviews the test results and certifies the control. Complete these steps:

1. Select **Control Testing > Controls** from the menu. The Controls window appears.
2. In the Controls table, click the Row Action icon () to access the action menu, and select **Create Certification**. The Create Control Certification window appears.
3. Select the certification period in the **Certification Period** drop-down list.
4. Select **Effectiveness** in the **Certification Measure** drop-down list.
5. Select **Effective** in the **Certification** drop-down list.
6. Enter *Passed all control tests* in the **Justification** field.
7. To link the control to the passed test, in the Referenced Tests table, click **Add Tests**, select the network firewall test, and click **Add and Close**.
8. Click **Certify**. The control is now certified for the certification period that you selected.
9. Log off from SAS Enterprise GRC.

Chapter 11

Implementing Audit Missions

Overview	123
Audit Missions and Audit Workflows	124
Overview	124
Roles for Audit Management	125
Audit Mission Lifecycle	125
Implementing an Example Audit Mission	127
Example Audit Management Process	127
Example: Audit Team Lead Creates the Audit Mission	128
Example: Audit Manager Approves the Audit Mission	129
Example: Local Business Manager Approves the Audit Mission	130
Example: Audit Team Lead Publishes the Audit Mission Tests	130
Example: Internal Auditor Accepts and Completes the Audit Mission	131
Example: Test Results Approver Approves the Audit Test Results	131
Example: Audit Team Lead Approves the Audit Mission	131

Overview

In SAS Enterprise GRC, an *audit* refers to the formal examination and evaluation of an organization's controls to ensure organizational compliance. The goal of audit management is to define audit missions and regularly test and evaluate the readiness of controls through an objective audit cycle.

Enterprise GRC enables you to maintain the objectivity of the audit process through access control. For example, a local business manager does not have access to information in the user interface about the auditors or the exact time of the audit. This helps prevent collusion or audit anomalies.

Lifecycle management is achieved through workflow stages that follow the audit business process. The following workflow stages exist by default:

- Create
 - The audit mission is created and saved, then sent for approval.
- Approve
 - The audit mission is approved by the audit manager and the local business manager.
- Audit

Audit tests are published and sent to the appropriate auditors, who conduct tests using the control testing process. See [“Implementing Controls and Control Tests” on page 111](#) for more information about the control testing process.

An audit mission can contain multiple tests. The results of each individual test are submitted and approved.

- Approve Audit

The overall audit mission is reviewed and approved.

- Fully Approved

The audit mission is fully approved.

The audit management workflow enables accountability and creates a traceable information stream for reporting purposes.

This chapter is primarily intended for users who participate in audit creation and management and enter data by means of the graphical user interface. For more information about the roles that participate in the audit management process, see [Table 11.1 on page 125](#).

This chapter uses the example of Orion Star, a bank that is using SAS Enterprise GRC to manage its GRC activities, and wants to administer audits through the system. The example uses the default SAS Enterprise GRC user interface environment and default workflow, and assumes that you have completed steps in previous chapters to implement the business structure, assign users to roles, and so on. It also assumes you understand the workflows for managing audit missions for this example. For more information about this example, see [Chapter 3, “Gathering Governance, Risk, and Compliance Data,” on page 27](#).

For more information about the default audit management workflows, see the *SAS Enterprise GRC: Workflow Administration Guide*.

Audit Missions and Audit Workflows

Overview

SAS Enterprise GRC enables the process of managing audit missions through the **Audits** menu. This menu enables you to perform the following tasks:

- Manage audit missions through the **Audit Missions** submenu.

You must have Audit capabilities assigned to manage the **Audit Missions** submenu.

- Manage controls through the **Controls** submenu. You can use this area to create and edit controls.

You must have Control capabilities assigned to manage the **Controls** submenu.

- Filter and view audit plans through the **Audit Planning** submenu.

You must have Audit capabilities assigned to manage the **Audit Planning** submenu.

- Manage test definitions and tests through the **Test Definitions** and **Tests** submenus. Tests are mechanisms to assess controls for a specific time period. A test contains exactly one control. A test definition is a template that is used for creating tests, and can contain multiple controls.

This testing mechanism functions in much the same way as control testing. For more information about control testing, see [“Implementing Controls and Control Tests” on page 111](#).

You must have Test Definition capabilities to manage the **Test Definitions** submenu.

- Manage control testing measures through the **Libraries** submenu. For more information about these items, see [“Control and Control Testing Definitions” on page 112](#).

The **Libraries** submenu is always available when users have the capability to access the **Audits** menu.

The management of audit workflows is completed through SAS Workflow Studio. For more information about audit workflows and using the SAS Workflow Studio, see the *SAS Enterprise GRC: Workflow Administration Guide*.

Roles for Audit Management

Capabilities to plan and manage audit missions are assigned through roles. The following table describes each role as it pertains to audit management.

Table 11.1 Roles for Audit Management

Role	Description
Enterprise GRC: Administration	Administrator. Administers the SAS Enterprise GRC environment. Might have responsibilities for maintaining audit workflows.
Enterprise GRC: Audit Team Leadership	Audit Team Lead. Responsible for the creation, ownership, and administration of audit missions.
Enterprise GRC: Audit Management	Audit Manager. Responsible for approving audit scope.
Enterprise GRC: Local Business Management	Local Business Manager. Responsible for approving audit scope.
Enterprise GRC: Auditing	Internal Auditor. Responsible for performing audit tests.
Enterprise GRC: Audit Tests Approval	Audit Tests Approver. Responsible for approving audit test results.
Enterprise GRC: Control Ownership	Control Owner. Responsible for approval of audit test results. Also has responsibilities for creating and maintaining controls.

Note: Depending on the capabilities of your assigned role, certain objects and fields in the user interface might be disabled for you during the completion of a task.

Audit Mission Lifecycle

The default audit management lifecycle is completed using the following steps:

1. The Administrator works with the Audit Team Lead, Audit Manager, Local Business Manager, Control Owner, and Internal Auditors to initially define the following in SAS Enterprise GRC:

- controls
- audit and control testing workflows
- control testing measures
- test definitions
- tests
- test periods

Note: Test definitions that are created under the **Audits** menu are visible only to those users with the Audit Management global permission.

Responsibilities are also assigned to any users during this step.

2. The Audit Team Lead creates the audit mission and provides details about the audit mission.

Depending on the management organization, the audit mission is then assigned to one or more Audit Team Leads, Audit Managers, and Local Business Managers.

The Audit Team Lead also assigns Internal Auditors for the tests specified in the audit mission.

The Audit Team Lead has the option to link the audit to other business objects, attach files or links, or add comments. The Audit Team Lead then sends the audit mission for approval.

3. The Audit Manager reviews the audit and approves the audit mission.
4. The Local Business Manager reviews the audit and approves the audit mission.
5. The Audit Team Lead publishes the tests specified in the audit.
6. Internal Auditors accept the tests, conduct tests and complete the audit.
7. Audit Tests Approvers approve the results of the audit test.
8. (If necessary) Control Owners approve the results of the audit test. The test results are now fully approved.
9. The Audit Team Lead reviews the fully approved tests and signs off that the audit mission is complete. The audit mission is now Fully Approved.

Tests created within the audit mission are only publicly viewable after the audit mission is fully approved. This maintains the secrecy of the audit proceedings.

Note: The Audit Team Lead has the option to approve the audit mission as long as the test results are submitted, even if the tests are not fully approved. This is called mission-level approval.

10. If needed, new audit missions can then be created from old audit missions.

Implementing an Example Audit Mission

Example Audit Management Process

The Investment Banking division at Orion Star is rolling out their GRC infrastructure. The division conducts regular audits and is using SAS Enterprise GRC to manage and track audits. For the purpose of this example, the following table displays the users involved in a specific type of audit. The responsibilities and roles that you define vary depending on your organization.

Table 11.2 Example Audit Mission Users and Roles

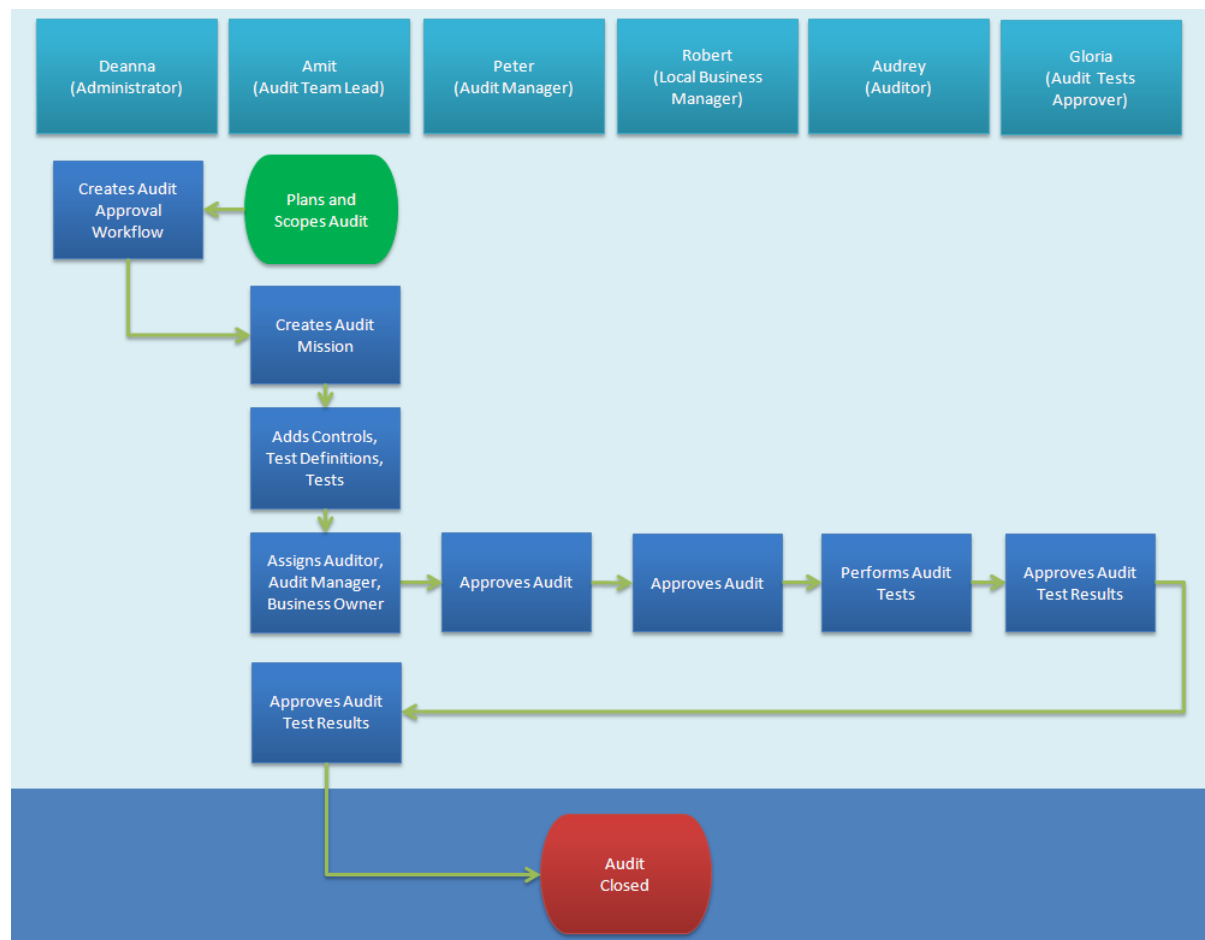
User	Job Title	SAS Enterprise GRC Roles
Deanna Tiswell	Administrator	Enterprise GRC: Administration
Amit Mohindra	Audit Team Lead	Enterprise GRC: Audit Team Leadership
Peter Baker	Audit Manager	Enterprise GRC: Audit Management
Audrey Speer	Internal Auditor	Enterprise GRC: Auditing
Robert Fitzgerald	Securities Department Risk Manager	Enterprise GRC: Local Business Management Enterprise GRC: Control Ownership
Gloria Hyatt	Investment Banking Division Expert	Enterprise GRC: Audit Tests Approval

The internal audit team conducts regular audits of the IT security infrastructure. Their mission is to periodically conduct an objective audit of the Investment Banking division to ensure that IT security controls are working as certified.

In this example, the internal audit management team is testing the example network firewall as specified in the control testing chapter. Although the control has been certified by the internal control testing team, the internal audit management team is verifying the control works as maintained.

This specific example assumes that the sample control and test definition have been created, and that the default workflow processes are in place. See [“Example Control Testing Process” on page 115](#) for more information about creating this sample control and test definition.

The following figure describes the business process for the example of Orion Star.

Display 11.1 Audit Mission Business Process Example

The example follows these steps:

1. Amit, the Audit Team Lead, [creates the audit mission](#).
2. Peter, the Audit Manager, [approves the audit mission](#).
3. Robert, as Local Business Manager, [approves the audit mission](#).
4. Amit, the Audit Team Lead, [publishes the audit tests](#).
5. Audrey, the Internal Auditor, [accepts the tests, completes the tests, and submits the audit test results](#).
6. Gloria, as Audit Tests Approver, [approves the audit test results](#).
7. Amit, the Audit Team Lead, [approves the audit mission](#).

Example: Audit Team Lead Creates the Audit Mission

Amit creates a new audit mission as Audit Team Lead. Complete these steps as Amit:

1. Select **Audits > Audit Missions** from the menu. The Audit Missions window appears.
2. Click **Create Audit Mission**. The Create Audit Mission window appears.
3. On the **Details** tab, enter the details of the audit mission. Complete these steps:

- a. Select the operational area for the audit mission. In the OL chooser, click **Edit**. In the Operational Area window, select the following dimensions and nodes from the Dimension drop-down list and click **Add** for each.
 - Dimension: **Management Organization**
 Node: **Management Organizations > iFinance > Investment Banking**
 Click **OK** to add the operational area and return to the previous window.
 - b. Enter *Network security audit* for the **Audit Title**.
 - c. Enter *Testing the network security of the Investment Banking division* as the **Audit Description**.
 - d. Select the date range for which the audit mission is planned. Provide an appropriate start date in the **Planned Start Date** and an appropriate end date in the **Planned End Date** fields.
 - e. Enter *Ensure that the network security is up to organizational standards.* in the **Audit Objective** field.
 - f. Enter *Annual audit testing* in the **Reason for Audit** field.
 - g. (Optional) Enter the detailed procedure for the audit in the **Audit Procedure** field. An option also enables you to attach the detailed procedure for the audit using the **Attachments** tab.
 - h. The audit has not been started, but airfare costs for the auditor have already been paid for. Expand **Related Costs**, and in the Costs table, click **Create Cost**. The Create Cost window appears.
 - i. Enter *Auditing airfare* as the **Description**.
 - j. Select **Airfare** in the **Cost Type** field.
 - k. The cost of airfare for the auditor was \$1500. Enter *1500* as the **Cost Amount** and select **USD** in the currency drop-down list. Click **OK** to close the Create Cost window.
4. On the **Resources** tab, view the Audit Team Leadership, Audit Management, and Local Business Management tables. Amit should be in the Audit Team Leadership table, Peter should appear in Audit Management, and Robert should appear in Local Business Management.
 5. On the **Scope** tab, enter control information. In the Controls table, click **Add Controls**. Select **IT Systems > Review and update the systems security infrastructure**, and click **Add and Close**.
 6. The example assumes that no attachments are needed for the audit mission. However, you can click on the **Attachments** tab should the audit mission exist in another document format. Also, you can click on the **Comments** tab to add comments or the **Related Content** tab to link the audit mission to one or more business objects.
 7. Click **Apply** to apply changes to the audit mission, and then click **Send for Approval** to send the audit mission to the Audit Manager for approval.
 8. Log off from SAS Enterprise GRC.

Example: Audit Manager Approves the Audit Mission

Peter approves the audit mission as Audit Manager. Complete these steps as Peter:

1. Select **Audits > Audit Missions** from the menu. The Audit Missions window appears.
2. Click on the network security audit. The View Audit Mission window appears.
3. Review the details of the audit. Peter is satisfied that the new audit covers all criteria. Click **Approve**, enter a **Change Reason**, and click **Save**. The Local Business Manager is notified that the audit mission has been approved.
4. Log off from SAS Enterprise GRC.

Example: Local Business Manager Approves the Audit Mission

Robert approves the audit mission as Local Business Manager. Complete these steps as Robert:


1. Select **Audits > Audit Missions** from the menu. The Audit Missions window appears.
2. Click on the network security audit. The View Audit Mission window appears.
3. Review the details of the audit. Note that some audit details, such as the scope of the audit and the names of the auditors, are hidden from Robert, to maintain the secrecy of the audit proceedings. This information is shown to the Local Business Manager only after the audit mission is fully approved.

Robert is satisfied that the audit mission covers all criteria. Click **Approve**, enter a **Change Reason**, and click **Save**. The Audit Team Lead is notified that the audit has been approved.

4. Log off from SAS Enterprise GRC.

Example: Audit Team Lead Publishes the Audit Mission Tests

Amit publishes the audit tests as Audit Team Lead. Complete these steps as Amit:

1. Select **Audits > Audit Missions** from the menu. The Audit Missions window appears.
2. Click on the network security audit. The Edit Audit Mission window appears.
3. On the **Resources** tab, in the Auditors table, click **Link Auditors** and select Audrey. Click **Add and Close**.
4. On the **Scope** tab, complete these steps:
 - a. In the Controls table, click the Create Tests From icon (). Select the network firewall test definition, and click **Create Tests**. The Create Tests from Audit Mission window appears.
 - b. On the Create Tests from Audit Mission window, leave the default test details, and then click **OK** to return to the **Scope** tab.
 - c. In the Tests table, select the test that you created, and click **Assign Auditors**. Select Audrey, and then click **Assign**.
5. Click **Publish Tests**. The Internal Auditor is notified that the audit tests have been published.
6. Log off from SAS Enterprise GRC.

Example: Internal Auditor Accepts and Completes the Audit Mission

Audrey accepts the new audit test as Internal Auditor, completes the audit mission, and submits the results. If the audit test contained multiple auditors, Audrey would have to first click **Accept** to accept the test, and then complete the audit. This enables auditors to pull from a pool of assigned tests. However, because Audrey is the only auditor assigned to the test, this step is automatically skipped by the system.

Complete these steps as Audrey:

1. Select **Audits > Audit Missions** from the menu. The Audit Missions window appears.
2. Click on the network security audit. The View Audit Mission window appears.
3. On the **My Tests** tab, in the Tests table, click on an attribute of the test. The Edit Test window appears.
4. Audrey runs the test on the control, the network firewall device. (For more information about this specific control test example, see [“Implementing an Example Control Test” on page 115](#).) When Audrey boots the firewall device, the redundant firewall device works as it should. She does the same on the redundant device, and it performs a fail over correctly. She repeats this test five times, and it does not fail. The audit was successful.

On the **Test Details** tab, enter information about the test results. In the **Test Results** area of the window, enter the following information:

- **Test Sample Description:** Enter *Performed reboot cycle 5 times*.
 - **Sample Size:** Select **Number**.
 - **Actual Sample Size:** Enter *5*.
 - **Actual Sample Failed:** Enter *0*.
5. On the **Responses** tab, the control measures Effectiveness. Select **Effective**.
 6. Click **Send for Approval**, enter a **Change Reason**, and click **Save**. The Test Results Approver is notified that the audit tests have been completed.
 7. Log off from SAS Enterprise GRC.

Example: Test Results Approver Approves the Audit Test Results

Gloria approves the test results. Complete these steps as Gloria:

1. Select **Audits > Tests** from the menu. The Tests window appears.
2. Click on the test related to the network security audit. The View Test window appears.
3. Review the details of the audit test. Gloria is satisfied with the test outcome. Click **Approve**, enter a **Change Reason**, and click **Save**. The test is now fully approved.
4. Log off from SAS Enterprise GRC.

Example: Audit Team Lead Approves the Audit Mission

Amit approves the audit mission as Audit Team Lead. Complete these steps as Amit:

1. Select **Audits > Audit Missions** from the menu. The Audit Missions window appears.
2. Click on the network security audit. The Edit Audit Mission window appears.
3. Review the details of the audit mission. Amit is satisfied with the test outcome. Click **Test Level Approval**, enter a **Change Reason**, and click **Save**. The audit mission is now fully approved.

Note: Amit can also select **Mission Level Approval** to fully approve the audit. **Test Level Approval** requires that all test results have been both submitted and fully approved. **Mission Level Approval** only requires that all test results have been submitted.

4. Log off from SAS Enterprise GRC.

Chapter 12

Implementing Scenarios and Scenario Workflows

Overview	133
Scenarios and Scenario Workflows	134
Overview	134
Roles for Scenarios	134
Scenario Process	135
Implementing an Example Scenario Assessment	136
Example Scenario	136
Example: Administrator Creates the Scenario Workflow	138
Example: Administrator Creates the Scenario Template	139
Example: Assessment Coordinator Creates Scenario	140
Example: Central Risk Manager Creates the Scenario Topic	141
Example: Assessor Completes the Scenario Questionnaire	141
Example: Scenario Validator Approves the Scenario Responses	142
Example: Business Owner Reviews and Closes the Scenario	142

Overview

Risk managers use *scenarios* to assess the potential extent and impact of future risk events. For example, a fire at a major location could have a huge impact on an organization's ability to conduct business. Such an event could result in power outages, damage or destruction of assets, injury to employees, or other devastating results.

To account for these events, risk managers create scenario questionnaires and send them to the appropriate employees so that these future risk events can be assessed.

Understanding and reviewing these scenarios help risk managers prepare for rare, catastrophic risks as well as assess the frequency and distributions of other risks. The process can also aid in the development of business continuity and disaster recovery plans.

Risk managers can also group scenarios together by *scenario topic* to help coordinate and report on overall strategies for dealing with risk events that might be related.

This chapter uses the example of Orion Star, a bank that is using SAS Enterprise GRC to manage its GRC activities. The example uses the default SAS Enterprise GRC user interface environment, and assumes that data has already been gathered about scenario workflows, users have been assigned to the appropriate roles, and that scenario questionnaires are either developed or are in development. For more information about this example, see [Chapter 3, “Gathering Governance, Risk, and Compliance Data,”](#) on [page 27](#).

Note: Your user interface might vary depending on the level of customization.

Scenarios and Scenario Workflows

Overview

SAS Enterprise GRC enables the process of creating scenarios and scenario workflows through the **Scenarios** menu. This menu enables you to perform the following tasks:

- Manage scenario topics through the **Scenario Topics** submenu.
You must have Scenario Topic capabilities to manage the **Scenario Topics** submenu.
- Manage scenarios through the **Scenarios** submenu.
You must have Assessment/Scenario capabilities to manage the **Scenarios** submenu.
- Manage scenario templates through the **Scenario Templates**. Scenario templates are used for creating scenarios. You can create multiple scenarios through a scenario template.
You must have Questionnaire/Scenario Template capabilities to manage the **Scenario Templates** submenu.
- Manage scenario workflows through the **Scenario Validation Workflow** submenu.
You must have Create Validation Workflow and Update Validation Workflow capabilities to view the Scenario Validation Workflow submenu.

Roles for Scenarios

Capabilities to manage scenarios are assigned through roles. The following table describes each role as it pertains to scenarios.

Table 12.1 Roles for Scenarios

Role	Description
Enterprise GRC: Administration	Administrator. Administers the SAS Enterprise GRC environment. Might have responsibilities for maintaining scenario workflows.
Enterprise GRC: Assessment Coordination	Scenario Assessment Coordinator. Responsible for an entire scenario assessment. Also referred to as assessment owner. This person is not necessarily the person who initiates an assessment. Might also have responsibilities creating and maintaining assessment templates.
Enterprise GRC: Assessment	Assessor. Responsible for answering scenario questionnaires.
Enterprise GRC: Assessment Approval	Assessment Approver. Reviews and approves a scenario assessment.

Role	Description
Enterprise GRC: Business Ownership	Business Owner. Reviews and closes validated scenarios.
Enterprise GRC: Central Risk Management	Central Risk Manager. Oversees scenarios and links scenarios to scenario topics.

Scenario Process

The scenario process is completed using the following steps:

1. The Administrator works with the Risk Manager, Assessment Coordinator, Business Owner, and Central Risk Manager to initially create and define the following in SAS Enterprise GRC:

- scenario templates

Scenario templates define the risk event type, the operational area, and the questionnaire. A template can be used for multiple scenarios. There are two approaches to define scenario templates: bucketed and rare event.

A bucketed scenario template asks for the expected frequency of losses for multiple severity ranges. For example, one bucket could have a severity range from \$0 up to \$10,000 in losses and some annual expected frequency of occurrence; another bucket could have a range of \$10,000 to \$50,000 and a different frequency; and a third bucket could range from \$50,000 to \$250,000 and have a third frequency.

A rare event scenario is intended to capture information about how often an extreme event happens, and what the expected impact range is. A rare event scenario template also asks for the minimum severity and maximum severity.

- scenarios

The scenario specifies the operational area, scenario template, and the positions that receive the scenario questionnaire. The scenario templates and positions that you can select are determined by the operational area of the scenario. All users who hold a position that you select and who have the Update Assessment and Scenario Questionnaire capabilities are scenario assessors. You can select additional users to receive a notification of the questionnaire. You must have at least one risk instance defined that matches both the risk event type of the corresponding scenario template and the scope of the selected positions.

- scenario topics
- scenario validation workflows
- scenario assessment periods
- scenario assessment questions and questionnaires

In addition, the following roles are assigned to different objects to manage scenarios, scenario topics, and scenario templates, to periodically complete scenario questionnaires, to validate scenario assessments, and to review the assessments:

- Assessment Coordinators
- Validators
- Assessors

- Business Owners
- Central Risk Managers

Following the initial setup, scenarios are typically managed by the Assessment Coordinator.

2. The Assessment Coordinator creates a scenario using the scenario template. The coordinator assigns an Assessor to the scenario, and opens the scenario. The scenario status is now Open.

A scenario must be opened before you can send the questionnaires to the assessors.

3. The Central Risk Manager creates a scenario topic. The risk manager links the scenario to the scenario topic.

Although you can create a scenario topic before you link the topic to the scenario, a scenario must be created before you can link a scenario to a scenario topic. One or more scenarios can be tied to a scenario topic.

4. Assessors answer the scenario questionnaires and submit the scenario for validation.

Multiple users can be assessors. Therefore, it is possible for multiple users to receive the same questionnaire. After one assessor submits responses for validation, other assessors can no longer see the questionnaire. Users that were chosen to receive a notification of the questionnaire can always see the questionnaire.

5. Validators review the information and validate the scenario, or return the scenario to the assessor to re-evaluate.

Validation occurs according to the defined validation workflow. A validator can either validate the responses or return them for correction. After responses are validated, they go to the next stage in the validation workflow. A validator cannot accept some responses and reject others on the same questionnaire. Within each questionnaire, all responses must be validated or returned together.

An assessor is notified on the task list when a response is returned to them. The assessor receives no explanation for the return. The validator should communicate the reasons to the assessor offline so that corrections can be made.

6. After the scenario has been validated, the Business Owner reviews and closes the scenario. The scenario status is now Closed.

Implementing an Example Scenario Assessment

Example Scenario

The securities department at Orion Star is rolling out their risk management infrastructure, and is implementing scenarios to understand the frequency of some possible risks within their organization. For the purpose of this example, the following table displays the users involved in scenarios and their job titles and roles. The responsibilities and roles that you define vary depending on your organization.

Table 12.2 Example Scenario Assessment Users and Roles

User	Job Title	SAS Enterprise GRC Roles
Deanna Tiswell	Administrator	Enterprise GRC: Administration
Samantha Glass	Risk Coordinator	Enterprise GRC: Assessment Coordinator
Robert Fitzgerald	Securities Department Risk Manager	Enterprise GRC: Assessment
Gloria Hyatt	Investment Banking Division Expert	Enterprise GRC: Assessment Approval
Jacques Simon	Central Operational Risk Manager, Investment Banking	Enterprise GRC: Business Ownership Enterprise GRC: Central Risk Management

In this example, the risk management team at Orion Star has a process to annually assess potential losses due to unmatched trades for the Securities group in the United States. Robert assesses this risk using a scenario questionnaire. Robert, the Risk Manager, has three severity buckets to assess the frequency of potential losses due to this risk: USD 0 to USD 10,000; USD 10,000 to USD 50,000; and USD 50,000 to USD 250,000. Any losses above this level would constitute a rare event, and are thus excluded from this scenario. The assets in question under this scenario are under the purview of the Investment Banking Division. Therefore, Jacques Simon is the business owner.

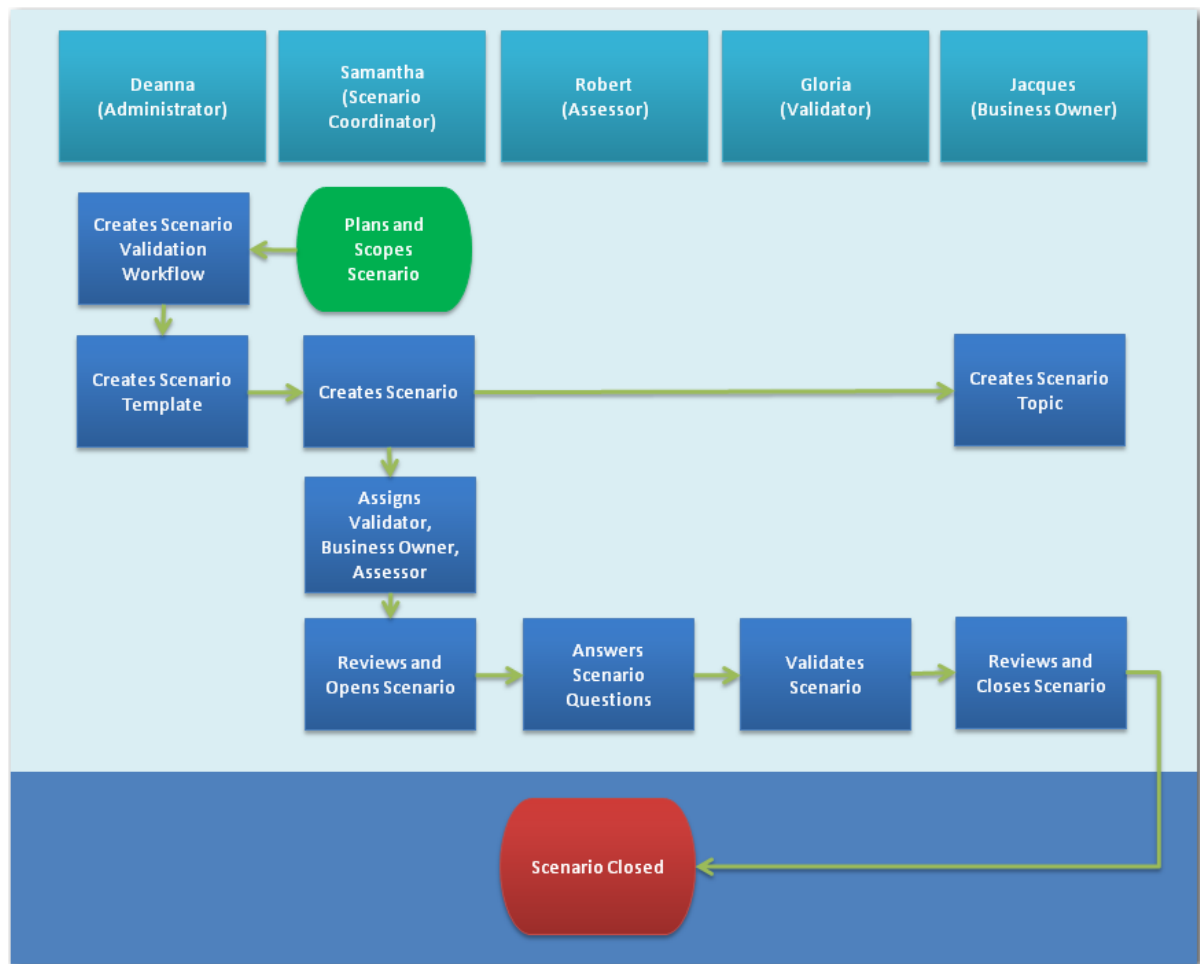
The Administrator, Deanna, works with Samantha, the Risk Coordinator, to create the scenario validation workflow and the scenario template.

The Risk Coordinator, Samantha, creates the scenario from the template, and assigns this scenario to Robert to answer questions about the potential for this risk within the group, and to enumerate the frequency of these losses. Robert's answers might come from historical information, such as internal company data or consortium data.

After the scenario has been created, Jacques creates a scenario topic and links the scenario to the scenario topic.

The questions are reviewed and validated by Gloria, an expert in the investment banking division. This example uses a one-stage validation workflow. When completed, Jacques, the Central Operational Risk Manager, reviews the scenario for decision-making purposes, and closes the scenario.

The following figure describes the business process for the example of Orion Star.

Display 12.1 Scenario Business Process Example

The scenario assessment example follows these steps:

1. Deanna, the Administrator, *creates the initial scenario validation workflow*.
2. Deanna *creates the scenario template*.
3. Samantha, the Assessment Coordinator, *creates the scenario and opens the assessment for completion*.
4. Jacques, the Central Risk Manager, creates the scenario topic and links the scenario to the scenario topic.
5. Robert, the Assessor, *completes the scenario questionnaire*.
6. Gloria, the Assessment Validator, *validates the completed scenario questionnaire*.
7. Jacques, the Business Owner, *reviews the responses and closes the scenario*.

Example: Administrator Creates the Scenario Workflow

Deanna, the Administrator, creates the initial scenario validation workflow. Complete these steps as Deanna:

1. Select **Scenarios > Scenario Validation Workflow** from the menu. The Scenario Validation Workflow window appears.

2. Select the operational area for the scenario. In the OL chooser, click **Edit** and in the Operational Point window, select the following dimensions and nodes from the Dimension drop-down list and click **Add** for each.
 - Dimension: **Management Organization**
Node: **Management Organizations > iFinance > Investment Banking > Securities**
 - Dimension: **Geography**
Node: **Geographies > Americas > North America > United States**
 Click **OK** to add the operational point and return to the previous window.
3. In the Current Validation Stages table, click **Edit Validation Stages**. The Edit Validation Stages window appears.
4. Click **Add Validation Stage**. The Add Validation Stage window appears.
5. Enter the name of the validation stage, *Validation Stage for Securities Department*, in the **Name** field.
6. Click **Add User**. The View Users window appears. Select Gloria as the Validator and return to the Add Validation Stage window.
7. Click **OK** to return to the Edit Validation Stages window.
8. This validation does not require multiple validation stages. Click **Save**, enter a reason for the change in the Change Reason window, and click **Save** again.

Example: Administrator Creates the Scenario Template

Deanna creates the scenario template as Administrator. Complete these steps as Deanna:

1. Select **Scenarios > Scenario Templates** from the menu. The Scenario Templates window appears.
2. Click **Create Scenario Template**. The scenario template wizard opens.
3. In the Details window, enter *How often do unmatched trades occur in the following loss buckets?* in the **Name** field. Select **USD** in the **Currency** field. Keep all other defaults and click **Next**.
4. In the Risk Event Type window, select the node **Execution, Delivery and Process Management > Transaction Capture, Execution, and Maintenance**. Click **Next**.
5. In the Operational Area window, select the operational area for the scenario. In the OL chooser, click **Edit** and in the Operational Area window, select the following dimensions and nodes from the Dimension drop-down list, and click **Add** for each.
 - Dimension: **Management Organization**
Node: **Management Organizations > iFinance > Investment Banking > Securities**
 - Dimension: **Geography**
Node: **Geographies > Americas > North America > United States**
 Click **Next**.
6. In the Layout window, click **Define Buckets**. The Define Buckets window appears.

There are three buckets in this scenario: 0 to 10000, 10000 to 50000, and 50000 to 250000. Enter these ranges in the buckets provided. Click **Add** to return to the previous window.

7. Click **Next**. The Summary window appears.
8. In the field **Do you want to create a scenario from this template now?**, select **No**. Click **Finish** to exit the wizard.
9. Log off from SAS Enterprise GRC.

Example: Assessment Coordinator Creates Scenario

Samantha creates the scenario as Assessment Coordinator, and opens the assessment for completion. Complete these steps as Samantha:

1. Select **Scenarios > Scenarios** from the menu. The Scenarios window appears.
2. Click **Create Scenario**. The create scenario wizard opens. Click **Next**.
3. In the Details window, enter *Unmatched Trade Losses*. Select the appropriate assessment period, such as 2010, in the **Assessment Period** drop-down list. Enter a future due date for the assessment to be completed in the **Assessor Due Date** field, and click **Next**.
4. Enter the operational area for the scenario. In the OL chooser, click **Edit**. In the Operational Area window, select the following dimensions and nodes from the Dimension drop-down list, and click **Add** for each.
 - Dimension: **Management Organization**
Node: **Management Organizations > iFinance > Investment Banking > Securities**
 - Dimension: **Geography**
Node: **Geographies > Americas > North America > United States**

Click **OK** to add the operational area and return to the previous window. Click **Next**.
5. In the Scenario Template window, select **How often do unmatched trades occur in the following loss buckets?**, and click **Next**.
6. In the Positions window, click the check box next to **Assessors**, the role that you want to perform the assessment, and click **Next**. The Notify List window appears.
7. In the Notify List window, you can choose to select any number of people to be notified when a change is made to the assessment. Add Jacques, the Business Owner, to the notify list. Jacques is notified of the assessment progress and when the assessment has been validated. He can then review and close the assessment. Click **Add User**. The View Users window appears. Click on the link for Jacques to select the user and return to the window. Click **Next**. The Summary window appears.
8. In the Summary window, select **Yes** for the option **Do you want to open the scenario now?**. Click **Finish** to exit the wizard. The Open Scenario window appears.
9. Click the check box next to **Assessor** role and click **Open**. The assessment is sent to Robert.
10. Log off from SAS Enterprise GRC.

Example: Central Risk Manager Creates the Scenario Topic


Jacques, the Central Risk Manager, creates the scenario topic. Complete these steps as Jacques:

1. Select **Scenarios > Scenario Topics** from the menu. The Scenario Topics window appears.
2. Click **Create Scenario Topic**. The Create Scenario Topic window appears.
3. On the **Details** tab, enter the operational area for the scenario topic. In the OL chooser, click **Edit**. In the Operational Area window, select the following dimensions and nodes from the Dimension drop-down list, and click **Add** for each.
 - Dimension: **Management Organization**
Node: **Management Organizations > iFinance > Investment Banking > Securities**
 - Dimension: **Geography**
Node: **Geographies > Americas > North America > United States**

Click **OK** to add the operational area and return to the previous window.
4. On the **Details** tab, enter *Trading Desk Scenarios* for the **Title**.
5. Enter *Scenarios related to Trading Desk operations* in the **Description** field.
6. Select **High** for the **Priority**.
7. On the **Scenarios** tab, link the scenario that you have created to the scenario topic. Click **Link Scenarios**. The Select Scenario Entries to Link window appears.
8. Select the scenario **Unmatched Trade Losses**, and click **Add and Close** to return to the Create Scenario Topic window.
9. Click **Save** to save the scenario topic.
10. Log off from SAS Enterprise GRC.


Example: Assessor Completes the Scenario Questionnaire

Robert, the Assessor, completes the scenario questionnaire. Complete these steps as Robert:

1. Select **Scenarios > Scenarios** from the menu. In the Scenarios table, click the Row Action icon () to access the action menu, and select **View Scenarios**. The Scenarios window appears. Click on the link in the Questionnaires table. In the scenario window, review the scenario assessment, and click **Begin Modification**.
2. Robert has observed that in the past year, there were 15 unmatched trade losses between \$0 and \$10,000, 6 unmatched trade losses between \$10,000 and \$50,000, and 3 unmatched trade loss between \$50,000 and \$250,000. Enter the numbers 15, 6, and 3 as frequencies for these buckets in the scenario questionnaire.
3. Click **Submit** to send the scenario to Gloria for validation.
4. Log off from SAS Enterprise GRC.


Example: Scenario Validator Approves the Scenario Responses

Gloria validates the scenario questionnaire. Complete these steps as Gloria:

1. Select **Scenarios > Scenarios** from the menu. In the Scenarios table, click the Row Action icon () to access the action menu, and select **View Scenarios**. The Scenarios window appears. Click on the link in the Questionnaires table. In the scenario window, review the scenario assessment answers, and click **Validate**.
2. Log off from SAS Enterprise GRC.

Example: Business Owner Reviews and Closes the Scenario

Jacques, the Business Owner, reviews the fully validated scenario for decision-making, and closes the scenario. Complete these steps as Jacques.

1. Jacques has received notifications that the scenario is now Fully Validated. Select **Scenarios > Scenarios** from the menu. The Scenarios window appears.
2. In the **Scenarios** table, click the down arrow icon () and select **Close**. The status of the scenario is now Closed.
3. Log off from SAS Enterprise GRC.

Chapter 13

Managing Risks and Implementing Assessments

Overview	144
Assessments and Assessment Workflows	145
Overview	145
Roles for Form-Based Assessments	146
Roles for Questionnaire-Based Assessments	147
Other Assessment-Related Roles	147
Form-Based Assessment Process	148
Questionnaire-Based Assessment Process	150
Direct-Edit Assessment Process	151
Defining Assessment Data Objects	151
Implementing Questionnaire-Based Risk and Control Assessments	152
Implementing Example Assessment Data Objects	153
Example Risk Creation Process	153
Example Risk Creation Steps	154
Example: Administrator Creates a New Risk	154
Example: Risk Owner Reviews and Approves the Risk	155
Example: Central Risk Manager Reviews and Fully Approves the Risk	155
Implementing an Example Form-Based Risk Assessment	156
Example Form-Based Assessment Process	156
Example Form-Based Assessment Steps	157
Example: Risk Assessment Coordinator Creates a New Form-Based Assessment	157
Example: Assessment Approver Reviews and Approves Form-Based Assessment Plan	159
Example: Assessor Reviews and Assesses the Risk	159
Example: Business Owner Responds to the Risk Results	160
Example: Assessment Approver Reviews and Approves the Assessment Completion	160
Implementing a Questionnaire-Based Risk Assessment	161
Example Questionnaire-Based Assessment Process	161
Example Questionnaire-Based Assessment Steps	162
Example: Administrator Creates the Questionnaire-Based Validation Workflow	163
Example: Risk Assessment Coordinator Links a Risk Event Type to a Question Group	163
Example: Risk Assessment Coordinator Creates a Questionnaire Template	164
Example: Risk Assessment Coordinator Creates a Questionnaire-Based Assessment	165
Example: Assessor Responds to the Risk Assessment Questionnaire	166

Example: Assessment Validator Reviews and Approves the Questionnaire-Based Assessment	166
Example: Business Owner Fully Validates and Closes the Questionnaire-Based Assessment	167

Overview

In SAS Enterprise GRC, risks, controls, causes, and potential impacts are referred to as *assessment items*, or *assessables*. The objective of the assessment process is to collect information about these assessment items and to evaluate them. This process involves sending questionnaires to the appropriate people within your organization and collecting their responses.

There is a difference between assessment items and *assessment item types*. Assessment item types are more general and identify a particular type of risk, cause, or control (there is no type associated to potential impacts). Assessment items (or instances) are formed when an assessment item type is associated with a particular operational location. For example, theft is a type of risk. In SAS Enterprise GRC, you can identify theft with an operational location such as the organization's investment banking division. This creates an assessment item, in this case a specific risk of theft in the investment banking division.

There are two types of process-related risk and control assessments: form-based assessments and questionnaire-based assessments. Both assessments are conducted in stages. Each stage requires a validation or sign-off before users can proceed to the subsequent stage. The main difference between these two assessment types is how questionnaires are handled. Form-based assessments add questionnaires as file attachments to form an optional pre-assessment that serves to support the assessment. The core assessment is performed at a later stage, using rating templates. Questionnaire-based assessments, however, incorporate questionnaire pages within the user interface that are designed to record the risk and control ratings. Questionnaire-based assessments require the creation of a separately defined questionnaire validation workflow. Form-based assessments are limited to one response form per assessment for all risks and controls, whereas questionnaires can assess these items separately.

Furthermore, form-based assessments enable the definition of follow-up actions, a management review and response, and automated integration with the issues and action plans.

Whether you conduct a form-based assessment or a questionnaire-based assessment, the assessment process includes a series of reviews and validations. This facilitates accountability and creates a traceable information stream for auditing and reporting purposes.

In addition to review and validation processes for form-based and questionnaire-based assessments, processes also exist for the creation of risks, controls, and potential impacts, which are integrated into the assessment process.

A third type of assessment, direct-edit, enables you to record risk ratings directly through the user interface without requiring a validation or sign-off process.

This chapter is primarily intended for users who participate in form-based and questionnaire-based risk assessments and enter data by means of the graphical user interface. For more information about the roles that participate in the assessment process, see [“Roles for Form-Based Assessments” on page 146](#) and [“Roles for Questionnaire-Based Assessments” on page 147](#).

This chapter uses the example of Orion Star, a bank that is using SAS Enterprise GRC to manage its GRC activities. The bank wants to use a risk assessment process to collect information about risks within its organization. The example uses the default SAS Enterprise GRC user interface environment. It assumes that you have completed steps in previous chapters to implement the business structure, assign users to roles, and so on. It also assumes that you understand the workflows for assessing risk for this example. For more information about this example, see [Chapter 3, “Gathering Governance, Risk, and Compliance Data,”](#) on page 27.

For information about the form-based assessment process, see [“Form-Based Assessment Process”](#) on page 148. For information about the questionnaire-based assessment process, see [“Questionnaire-Based Assessment Process”](#) on page 150.

For more information about scenario assessments, see [Chapter 12, “Implementing Scenarios and Scenario Workflows,”](#) on page 133.

You can customize the user interface to enable or disable assessment types. For more information about enabling or disabling assessments in the system configuration, see the *SAS Enterprise GRC: Administration and Customization Guide*.

Assessments and Assessment Workflows

Overview

SAS Enterprise GRC enables the process of managing assessment items and assessment workflows through the **Risk Management** menu. This menu enables you to perform the following tasks:

- Manage assessments through the **Assessments** submenu.
You must have Assessment capabilities assigned to manage the **Assessments** submenu.
- Manage risks through the **Risk Profile** submenu. A risk consists of an operational location and a type of risk event. The risk also contains information about risk ownership, and can be linked to a number of different objects, such as causes, controls, KRIs, and issues.
You must have Risk capabilities assigned to manage the **Risk Profile** submenu.
- Manage potential impacts through the **Impacts** submenu. An impact consists of an operational location and an amount associated with the impact. The impact can have an owner and can be linked to a number of different objects, such as recent assessments, risks, and issues.
You must have Impact capabilities assigned to manage the **Impacts** submenu.
- Manage controls through the **Controls** submenu. Similar to risks, a control consists of an operational location and a control type. The control can also be linked to a number of different objects, such as mitigated risks, KRIs, and tests.
You must have Control capabilities to manage the **Controls** submenu.
- Manage the assessment planning process through the **Assessment Planning** submenu. You can use this area to review past and future assessments and to prepare for new assessments. Note that the actual scheduling of assessments is done through the assessment and not through this window.

You must have Assessment capabilities to manage the **Assessment Planning** submenu.

- Manage the assessment validation process through the **Assessment Validation Workflow** submenu. You can use this area to create and modify the validation process used for questionnaire-based assessments.

You must have Validation Workflow capabilities assigned to manage the **Assessment Validation Workflow** submenu.

- Manage assessment item types and other objects related to the risk assessment process through the **Libraries** submenu.

The **Libraries** submenu is always available when users have capabilities to view the **Risk Management** menu.

Roles for Form-Based Assessments

Capabilities to manage form-based assessments are assigned through roles. The following table describes each role as it pertains to form-based assessments.

Table 13.1 Roles for Form-Based Assessments

Role	Description
Enterprise GRC: Administration	Administrator. Administers the SAS Enterprise GRC environment. Might have responsibilities for maintaining the assessment workflow and setting up the assessment libraries (risks, controls, causes, measures, response scales, rating groups, rating templates, assessment templates, and supportive questionnaires)
Enterprise GRC: Assessment Coordination	Assessment Coordinator. Responsible for an entire assessment. Also referred to as assessment owner. This person is not necessarily the person who initiates an assessment. Might also have responsibilities for maintaining the assessment libraries and performing direct edit assessments.
Enterprise GRC: Assessment Approval	Assessment Approver. Reviews and approves an assessment. For controls, the assessment ends after the assessment stage. For risks, the assessment ends after the Accept/Respond stage.
Enterprise GRC: Assessment	Assessor. Assigns ratings to assessments and proposes recommendations for the risks and controls that the assessment was designed to review.
Enterprise GRC: Business Ownership	Business Owner. Involved in risk assessments only and accepts or responds to risk ratings and recommendations in the final stage of the assessment.

Note: Depending on the capabilities of your assigned role, certain objects and fields in the user interface might be disabled for you during an assessment.

Roles for Questionnaire-Based Assessments

Capabilities to manage questionnaire-based assessments are assigned through roles. The following table describes each role as it pertains to questionnaire-based assessments.

Table 13.2 Roles for Questionnaire-Based Assessments

Role	Description
Enterprise GRC: Administration	Administrator. Administers the SAS Enterprise GRC environment. Might have responsibilities for maintaining the assessment workflow and setting up the assessment libraries (risks, controls, causes, measures, response scales, questions, question groups, and questionnaire templates).
Enterprise GRC: Assessment Coordination	Assessment Coordinator. Responsible for an entire assessment. Also referred to as assessment owner. This person is not necessarily the person who initiates an assessment. Might also have responsibilities for maintaining the assessment libraries and performing direct edit assessments.
Questionnaire Assessor	Assessor. Assigns ratings for the risks, controls, and causes that the questionnaire was designed to review. Although there is no default SAS Enterprise GRC role for this person, an assessor must have the View and Update capabilities for assessment questionnaires, and the View capability for assessments, risks, and controls. Assessment can be performed by a number of SAS Enterprise GRC roles.
Questionnaire Validator	Questionnaire Validator. Reviews and validates a questionnaire that has been submitted by an assessor or another validator who is earlier in the assessment validation workflow. There is no default SAS Enterprise GRC role for this person. For information about the assessment validation workflow, see “Defining Processes” on page 35 .

Note: Depending on the capabilities of your assigned role, certain objects and fields in the user interface might be disabled for you during an assessment.

Other Assessment-Related Roles

Other roles are optional and can play a part in the risk management and assessment process. These include the following:

Table 13.3 Other Assessment Roles

Role	Description
Assessment Questionnaire Respondent (Form-Based Assessments Only)	Completes any pre-assessment questionnaires. There is no default SAS Enterprise GRC role for this person.
Enterprise GRC: Assessment Questionnaire Approval (Form-Based Assessments Only)	Assessment Questionnaire Approver. Approves all completed pre-assessment questionnaires.
Enterprise GRC: Expert Area Reviewing	Reviewer. Reviews information submitted by an assessor. Each assessor can have a different set of reviewers.
Enterprise GRC: Expert Review Approval	Expert Review Approver. Approves all reviews of an assessor's submission. Each assessor can have a different reviewer approver.
Enterprise GRC: Risk Editing	Risk Editor or Risk Owner. Responsible for managing and editing risk profiles.
Enterprise GRC: Control Editing	Control Editor or Control Owner. Responsible for managing and editing controls.
Enterprise GRC: Risk Assessment Management	Risk Assessment Manager. Responsible for the overall risk assessment process. Assessment Coordinators typically report to this role.

Form-Based Assessment Process

The form-based assessment process is completed using the following steps:

1. The Administrator works with the Assessment Coordinator, Risk Owner, and Control Owner to initially define the following in SAS Enterprise GRC:
 - assessment item types
 - assessment items (risks, controls, and potential impacts)
 - assessment measures and response scales
 - assessment periods
 - rating groups
 - ratings templates
 - assessment templates
 - supportive questionnaires
 - assessment workflows

Note: Some of these objects are not defined through the user interface. For more information about loading or configuring these objects, see the *SAS Enterprise GRC: Administration and Customization Guide*.

Following the initial setup, an Assessment Coordinator typically manages and initiates risk assessments.

2. The Assessment Coordinator plans the risk assessment. Pre-assessment is an option that can be performed during this stage. Pre-assessment is similar to the assessment process in that supportive questionnaires are distributed, returned, and approved. Pre-assessment respondents receive an e-mail with a file attachment containing the supportive questionnaire. Any pre-assessment questionnaires must be returned before the assessment can continue to the scoping stage.

The Assessment Coordinator then assigns an Assessment Approver (to approve both the assessment plan and the completed assessment) and Assessors to the assessment. If the ratings template includes risk ratings, the Assessment Coordinator also assigns a Business Owner.

The coordinator has the option to pre-populate the assessment with risks, controls, and impacts for the assessors to review and select and distribute assessment questionnaires.

3. An Assessment Approver reviews and approves the assessment plan. After the approver has approved the plan, the assessment is now approved for assessors to complete.
4. Assessors perform the assessment. In this stage, Assessors can identify new risks/controls and delete pre-populated risks/controls as needed. After they have identified the risks/controls that they are assessing, they rate them and provide any justifications and recommendations. Assessors then sign off on their ratings. Other users can also review the risks/controls that have been signed off but can only add comments.

After Assessors sign off on their ratings, the information contained in the ratings for that assessment is considered frozen at the time of sign off. For example, any future changes to answer sheets are not reflected in the frozen answer sheets.

5. In a control assessment, the Assessment Owner (typically the Assessment Coordinator) sends the assessment again for approval, after which the assessment is complete. In a risk assessment (or a risk and control assessment), the Business Owner receives the assessment for acceptance.
6. If the assessment is related to a risk or risk and control assessment, the Business Owner accepts the risks or responds to them, specifies the issue owner for each risk, and then submits the assessment again for approval. Any new or changed risk/control profiles are saved.

In addition, an issue is created automatically for each risk decision that was provided by the business owner. If the business owner makes a recommendation, then an action plan for each mitigation action is created.

7. Assessment Approvers review the completed assessment and approve the assessment. By default, there is only one stage of approval.

SAS Enterprise GRC enables you to customize multiple stages of approval through SAS Workflow Studio.

After responses are approved, they are submitted to the next stage in the approval workflow. The submit-and-approve process repeats until the responses have been verified at all workflow stages. The assessment is now fully approved and closed.

After the assessment is closed, the information contained within the assessment is considered frozen at the time of the assessment. Future changes to assessment objects (such as triggers, information about the assessment frequency, questionnaires, and so on) are not reflected in the completed assessment.

Questionnaire-Based Assessment Process

A questionnaire-based assessment requires a separately defined validation workflow, similar to other objects in SAS Enterprise GRC (for example, scenarios).

Just as in the form-based assessment process, before you initiate a questionnaire-based assessment, you must define the data objects to be used in the assessment. You define some of these objects outside of SAS Enterprise GRC and then data load them into the application. You create others directly in the user interface. All of these objects, however, can be viewed and managed in libraries that you can access on the **Risk Management** menu.

The default questionnaire-based assessment process is completed using the following steps:

1. The Administrator works with the Assessment Coordinator, Risk Owner, and Control Owner to initially define the following in SAS Enterprise GRC:

- assessment item types
- assessment items (risks, controls, and causes)
- assessment measures and response scales
- assessment questions
- assessment periods
- question groups
- questionnaire templates
- assessment validation workflows

Note: Some of these objects are not defined through the user interface. For more information about loading or configuring these objects, see the *SAS Enterprise GRC: Administration and Customization Guide*.

Following the initial setup, an Assessment Coordinator typically manages risk assessments.

2. The Assessment Coordinator creates an assessment questionnaire template. This includes scoping the assessment and deciding which types of items to assess. The Assessment Coordinator also selects the specific question groups to include in the assessment. The question groups contain questions and response scales and are designed to evaluate assessment items (risk events, causes, and controls).
3. The Assessment Coordinator creates the risk assessment using the questionnaire template. The Assessment Coordinator then assigns questionnaires to positions within the organization to answer the questions.
4. Questionnaire Assessors perform the assessment by answering the questions within the questionnaire. Questionnaire Assessors then submit their answers for validation.
5. Questionnaire Validators review the completed assessment and validate the assessment. After responses are validated, they are submitted to the next stage in the validation workflow. The submit-and-validate process repeats until the responses have been verified at all workflow stages. The assessment is now fully validated and closed.

Note: Questionnaire-based assessments and form-based assessments use different workflow interfaces. Questionnaire-based assessments use a static workflow process that uses the SAS Enterprise GRC user interface, whereas form-based

assessments enable you to create dynamic workflows in the SAS Workflow Studio.

Direct-Edit Assessment Process

A third type of assessment, direct-edit, does not use a workflow process. Users rate risks independently of an assessment process.

The following data objects are used in direct-edit assessments:

- risks
- risk measures
- default response scales

The direct-edit risk assessment process is completed by an Assessment Coordinator, using the following steps:

1. The Assessment Coordinator selects the operational area to which the assessment applies. Setting the operational area filter is necessary to enter into direct-edit mode.
2. The Assessment Coordinator customizes the Risks table to include any risk measures to edit as needed.
3. The Assessment Coordinator selects the risks to assess and edits the risks (through the **Edit Selected Values** link).
4. The Assessment Coordinator selects the assessment period and provides values for the measures.
5. The Assessment Coordinator saves the values.

Defining Assessment Data Objects

Before initiating a form-based assessment or questionnaire-based assessment, you must define several data objects to be used in the assessment. You can define some of these objects outside of SAS Enterprise GRC and then data load them into the application. Others, you create directly in the user interface.

Risks, potential impacts, and controls can be viewed and managed from the **Risk Profile**, **Impacts**, and **Controls** submenus, respectively. These data objects are often created as part of the risk assessment process, and might not require definition before implementing risk assessments.

Other data objects can be viewed and managed on the **Libraries** submenu that you access from the **Risk Assessment** menu.

The following data objects are used for both form-based and questionnaire-based assessments:

- risk event types
- cause types
- control types
- measures
- response scales

The following data objects are used only in form-based assessments:

- ratings groups
- ratings templates
- assessment templates
- supportive questionnaires

The following data objects are used only in questionnaire-based assessments:

- questions
- question groups
- questionnaire templates

For more information about the procedures to create, load, modify, and remove these objects, see the *SAS Enterprise GRC: Help* or the *SAS Enterprise GRC: Administration and Customization Guide*.

Implementing Questionnaire-Based Risk and Control Assessments

A questionnaire-based assessment requires a separately defined validation workflow, similar to other objects in SAS Enterprise GRC (for example, scenarios).

Just as in the form-based assessment process, before you initiate a questionnaire-based assessment, you must define data objects to be used in the assessment. You define some of these objects outside of SAS Enterprise GRC and then data load them into the application. Others, you can create directly in the user interface. All of these objects, however, can be viewed and managed in libraries that you can access on the **Risk Management** menu. The following data objects are used in questionnaire-based assessments:

- cause, control, and risk event types
- question groups
- response scales
- measures

The questionnaire-based risk and control assessment process is completed using the following steps:

1. Create the assessment data objects, as needed.
2. Define the assessment validation workflow.
3. Create an assessment questionnaire template. You select the operational area to which the template applies and which types of items to assess at that operational location. You also select the specific question groups to include in the assessment. The question groups contain questions and response scales and are designed to evaluate assessment items (risk events, causes, and controls).
4. Create the assessment based on a questionnaire template. During assessment creation, you specify the positions in the organization to which to send questionnaires.
5. Open the assessment. You send the assessment questionnaires to the designated assessors, who respond to the questionnaires and submit their answers for validation.
6. Validate the assessment. The set of responses to the questionnaire enters the assessment validation workflow. After a questionnaire is submitted, a validator receives the responses and can either validate the responses or return them for correction. After responses are validated, they are submitted to the next stage in the

validation workflow. The submit-and-validate process repeats until the responses have been verified at all workflow stages.

7. Close the assessment and propagate the risk scores.

Implementing Example Assessment Data Objects

Example Risk Creation Process

The securities department at Orion Star is rolling out their GRC infrastructure, and is implementing a business process to create and assess risks, potential impacts, and controls. For the purpose of this example, the following table displays the users involved in creating risks and their job titles and roles. This business process can apply to controls and potential impacts as well as risks. The responsibilities and roles that you define vary depending on your organization.

Table 13.4 *Example Risk Creation Users and Roles*

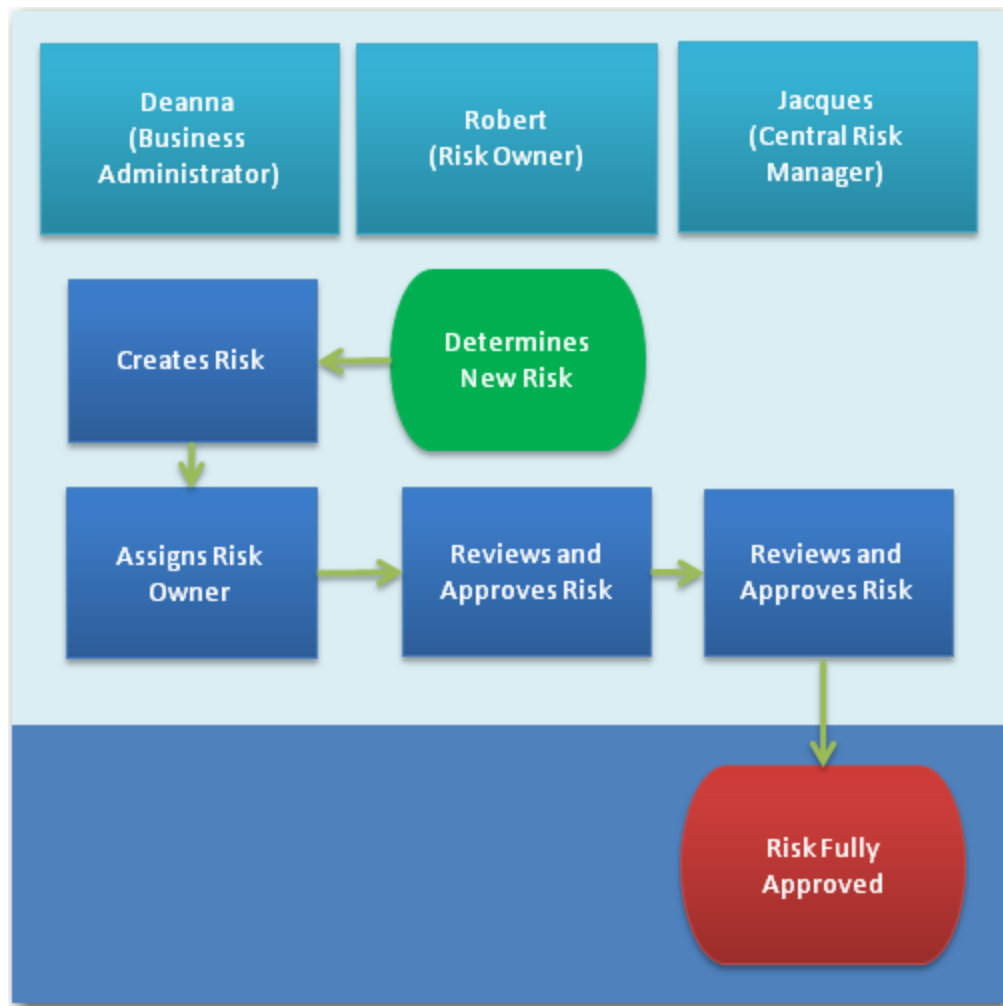
User	Job Title	SAS Enterprise GRC Roles
Deanna Tiswell	Administrator	Enterprise GRC: Administration
Robert Fitzgerald	Securities Department Risk Manager	Enterprise GRC: Local Risk Management
Jacques Simon	Central Operational Risk Manager, Investment Banking	Enterprise GRC: Central Risk Management

In this example, the IT Security group at Orion Star is aware of a new risk at the organization, the risk of internal fraud through the mismarking of positions. Assets under internal fraud risk are under the purview of the Securities Department. Therefore, Robert has accepted the risk as his own and has the role of Risk Owner. Ultimate ownership of risks to assets falls to the Central Risk Manager, Jacques.

Deanna, the Administrator, is creating the risk and assigning ownership of the risk to Robert. The risk entry is reviewed and approved by Robert and finally reviewed and approved by Jacques.

The following figure describes the business process for the example of Orion Star.

Display 13.1 Example Risk Creation Business Process at Orion Star



Example Risk Creation Steps



The risk creation example follows these steps:

1. Deanna, the Administrator, [creates a new risk on page 154](#).
2. Robert, the Risk Owner, [reviews and approves the new risk on page 155](#).
3. Jacques, the Central Risk Manager, [reviews and fully approves the new risk on page 155](#).

Example: Administrator Creates a New Risk

Deanna creates a new risk as Administrator. Complete these steps as Deanna:

1. Select **Risk Management > Risk Profile** from the menu. The Risk Profile window appears.
2. Click **Create Risk**. The Create Risk window appears.

3. Edit the operational area for the risk. In the OL chooser, click **Edit**. In the Operational Area window, select the following dimensions and nodes from the Dimension drop-down list, and click **Add** for each.
 - Dimension: **Management Organization**
Node: **Management Organizations > iFinance > Investment Banking > Securities**
 - Dimension: **Geography**
Node: **Geographies > Americas > North America > United States**
 Click **OK** to add the operational area and return to the previous window.
4. In the **Risk Title** field, enter *Mismarked Position Fraud*.
5. Robert is also the risk owner. Click the Select User icon () in the **Risk Owner** field. Select **Robert Fitzgerald** as the risk owner.
6. This risk is related to Sarbanes-Oxley regulations. In the **SOX Related** field, select **Yes**.
7. Select the identifier of the risk. Robert has identified the risk. Click the Select User icon () in the **Identified By** field. Select **Robert Fitzgerald** as the assessment owner.
8. Under **Risk Event Type**, select **Internal Risk Event Types > Internal Fraud > Unauthorized Activity > Mismarking of position (intentional)**.
9. Keep all other defaults, click **Apply**, and then click **Send for Approval** to send the risk to Robert for approval.
10. Log off from SAS Enterprise GRC.

Example: Risk Owner Reviews and Approves the Risk

Robert approves the new risk as Risk Owner. Complete these steps as Robert:

1. Robert has received notification via the task list that he needs to approve the new risk. Robert is satisfied with the risk. Click on the task link. On the View Risk window, review the risk, and click **Approve**. Enter a change reason, and click **Save**. The new risk is sent to Jacques for approval.
2. Log off from SAS Enterprise GRC.

Example: Central Risk Manager Reviews and Fully Approves the Risk

Jacques fully approves the risk as Central Risk Manager. Complete these steps as Jacques:

1. Jacques has received notification via the task list that he needs to approve the new risk. Jacques is satisfied with the risk. Click on the task link. On the assessment window, review the assessment, and click **Approve**. Enter a change reason, and click **Save**. The new risk is now fully approved.
2. Log off from SAS Enterprise GRC.

Implementing an Example Form-Based Risk Assessment

Example Form-Based Assessment Process

The securities department at Orion Star is rolling out their GRC infrastructure, and is implementing an assessment process to assess risks, potential impacts, and controls. For the purpose of this example, the following table displays the users involved in performing risk assessments and their job titles and roles. The responsibilities and roles that you define vary depending on your organization.

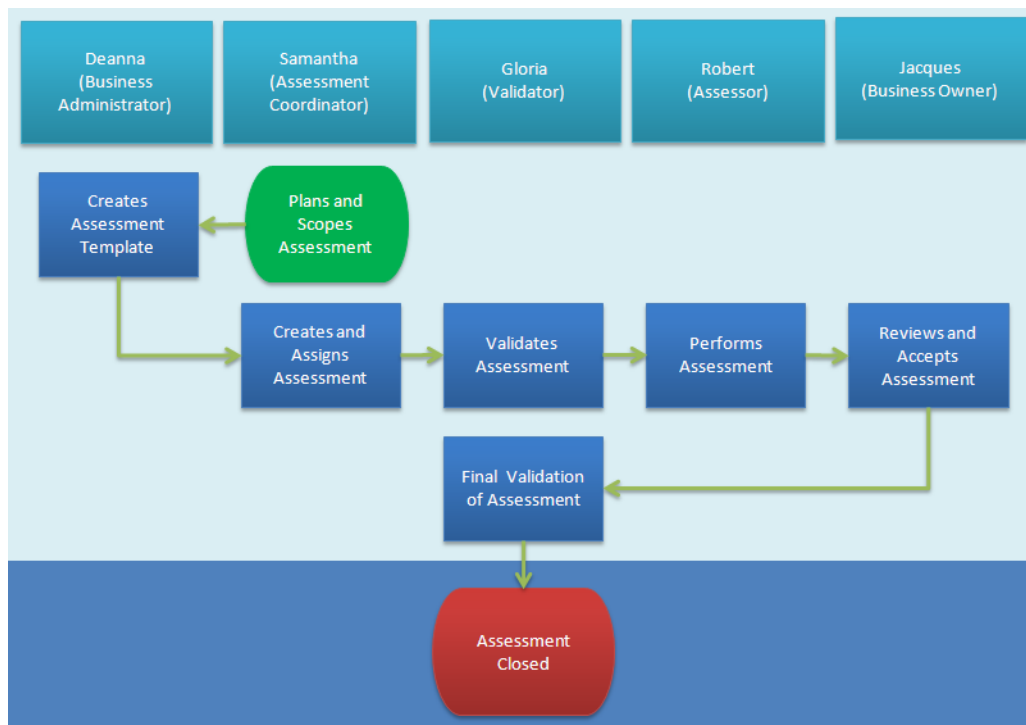
Table 13.5 Example Assessment Users and Roles

User	Job Title	SAS Enterprise GRC Roles
Deanna Tiswell	Administrator	Enterprise GRC: Administration
Robert Fitzgerald	Securities Department Risk Manager	Enterprise GRC: Assessment
Samantha Glass	Risk Coordinator	Enterprise GRC: Assessment Coordination
Jacques Simon	Central Operational Risk Manager, Investment Banking	Enterprise GRC: Business Ownership
Gloria Hyatt	Investment Banking Division Expert	Enterprise GRC: Assessment Approval

In this example, the IT Security group at Orion Star is assessing its risk of internal fraud. Assets under the threat of fraud are under the purview of the Securities Department. Therefore, Robert has the role of Assessor. Ultimate ownership of assets falls to the Central Risk Manager, Jacques, who is the Business Owner in this example.

The Risk Coordinator, Samantha, is planning to review risks on a quarterly basis. These assessments are completed by Robert, reviewed by Jacques, and validated by Gloria. This specific example uses a form-based assessment process.

The following figure describes the business process for the example of Orion Star.

Display 13.2 Example Form-Based Risk Assessment Business Process for Internal Fraud at Orion Star

The assessment process that follows assumes that the Administrator has already created the assessment data objects. For more information about creating the risk, see [“Example Risk Creation Process” on page 153](#). Other objects are already available as part of the sample data. Therefore, no additional steps are required. See [“Defining Assessment Data Objects” on page 151](#) for additional information.

Example Form-Based Assessment Steps





The form-based assessment example follows these steps:

1. Samantha, the Risk Assessment Coordinator, [creates a new assessment](#).
2. Gloria, the Assessment Approver, [approves the initial assessment plan](#).
3. Robert, the Assessor, [assesses the risk](#).
4. Jacques, the Business Owner, [responds to the risk results](#).
5. Gloria [approves the completed assessment](#).

Example: Risk Assessment Coordinator Creates a New Form-Based Assessment

Samantha creates a new assessment as Risk Assessment Coordinator. Complete these steps as Samantha:

1. Select **Risk Management > Assessments** from the menu. The Assessments window appears.
2. This assessment is form-based. Click **Create Assessment**, and select **Form-Based**. The Create Assessment window appears.

3. On the **Details** tab, complete these steps:
 - a. Edit the operational area for the control. In the OL chooser, click **Edit**. In the Operational Area window, select the following dimensions and nodes from the Dimension drop-down list, and click **Add** for each.
 - Dimension: **Management Organization**
Node: **Management Organizations > iFinance > Investment Banking > Securities**
 - Dimension: **Geography**
Node: **Geographies > Americas > North America > United States**
 Click **OK** to add the operational area and return to the previous window.
 - b. Enter *Internal Fraud* in the **Assessment Name** field.
 - c. Under **Assessment Type**, select **Operational**.
 - d. Under **Initiated By**, select **Operational**.
 - e. Elect not to perform a pre-assessment. Keep all other defaults, and click the **Schedule** tab.
4. On the **Schedule** tab, complete these steps:
 - a. Select the appropriate assessment time period in the **Assessment Period**.
 - b. Select the dates for which the assessment is planned. Provide an appropriate date in the **Planned Start Date** and **Planned End Date** fields. Also provide a due date for the assessor in the **Assessor Due Date** field.
 - c. Internal fraud is considered a medium risk to assets. Select **Medium** in the **Asset Risk Profile** field.
 - d. The risk is to be assessed every 6 months. Select **6 Months** in the **Assessment Frequency** field. Click the **Resources** tab.
5. On the **Resources** tab, complete these steps:
 - a. Select the assessment owner. It should already be Samantha Glass. If not, click the Select User icon () in the **Assessment Owner** field. Select **Samantha Glass** as the assessment owner.
 - b. In the **Validator** field, click the Select User icon () . Select **Gloria Hyatt** as the validator.
 - c. In the **Assessor** field, add any people who will participate in this assessment. Click **Add Assessor**, and select **Robert Fitzgerald** as the assessor. Click the **Scoping** tab.
6. On the **Scoping** tab, complete these steps:
 - a. Select **assmntTriggrrNm1** in the **Assessment Trigger** field.
 - b. The asset is assigned to the management organization. Select **Management Organization** in the **Asset** field.
 - c. The assessment uses a risk ratings template. In the **Ratings Template** field, click the Select Ratings Template icon () and select **Risk Ratings Template**.
 - d. In the **Business Owner** field that appears when you select this template, click the Select User icon () . Select **Jacques Simon** as the business owner.

- e. This risk assessment includes a step for the business owner to accept the assessment for final validation. Select **Yes** in the **Include Accept/Respond Stage** field.
7. Samantha has identified several types of internal fraud, but specifically has identified a risk that someone could intentionally mismark a position. Risks are pre-populated for this assessment. Click **Add Risk from Library**. The Select Risks window appears.
8. Select Robert as the **Assessor** for the risk.
9. Select the mismarked position fraud risk, and click **Add and Close**.
10. Click **Send for Validation** to send the assessment plan to Gloria for validation.
11. Log off from SAS Enterprise GRC.


Example: Assessment Approver Reviews and Approves Form-Based Assessment Plan

Gloria validates the initial assessment plan as Validator. Complete these steps as Gloria:

1. Gloria has received notification via the task list that she needs to validate the assessment. Gloria is satisfied with the assessment plan. Click on the task link. On the assessment window, review the assessment, and click **Validate**. Enter a change reason in the **Reason Text**, and click **Save**. The risk is sent to the Robert, the risk assessor.
2. Log off from SAS Enterprise GRC.

Example: Assessor Reviews and Assesses the Risk


Robert assesses the risk as Assessor. Complete these steps as Robert:

1. Robert has received notification via the task list that he needs to complete an assessment. Click on the task link. On the assessment window, click the **Ratings** tab, and click on the assessment link.
2. In the Risks table, click the down arrow icon  and select **Perform Rating**. The View Risk window appears.
3. This risk has a direct effect, an expected financial loss of \$250,000. Enter 250000 in the **Expected Financial Loss** field, and select **USD** as the currency.
4. The risk rating is considered medium. Select **Medium** in the **Direct Risk Rating** drop-down list.
5. The fraud is not expected to have any media coverage, although there is a small risk that this could occur. Select **Low** for each drop-down list for the following fields: **No External Media Coverage**, **Local Media Coverage**, **Regional Media Coverage**, and **National Media Coverage**.
6. Enter a justification for the overall risk rating, such as *Some financial impact, but low external impact*.
7. In the Recommendations table, click **Create Recommendation**. The Create Recommendation window appears.
8. Enter *Improve IT systems* in the **Recommendation Title**.

9. In the Mitigating Actions table, click **Create Mitigating Action**. The Create Mitigating Action window appears.
10. Enter *Improve IT system handling of position information* in the **Mitigating Action Description**. Click **OK**.
11. Select an appropriate **Target Completion Date** for the mitigating action.
12. Select **Low** for the **Risk Rating Post Mitigation**, and then click **OK** to return to the View Risk window.
13. Click **Save** to return to the Assessment window.
14. Click **Sign Off** to sign off on the assessment. The assessment goes to the Business Owner, Jacques Simon, to accept or respond to the risk results.
15. Log off from SAS Enterprise GRC.

Example: Business Owner Responds to the Risk Results

Jacques responds to the risk results as Business Owner. Complete these steps as Jacques:

1. Jacques has received notification via the task list that he needs to accept or respond to an assessment. Click on the task link. On the assessment window, review the assessment.
Click the **Accept/Respond** tab.
2. In the **Risks** table, click on the risk named **Mismarked positional fraud**. The View Risk window appears.
3. Jacques has decided to accept the risk. In the **Accept/Respond** table, in the **Response** field, select **Mitigate**.
4. In the Selected Recommendation table, click **Add Assessor Recommendation**. The Select Assessor Recommendation window appears.
5. In the **Risk Recommendation** field, click the Select Recommendation icon ().
Click the details about the recommendation for improving IT systems to select the recommendation, and then click **OK** to return to the View Risk window. When you provide a risk recommendation in an assessment, an issue and action plan is automatically created from it upon validation of the assessment.
6. Accept all other default information, and click **Save** to return to the Edit Assessment window.
7. Click **Send for Validation**. The assessment is sent to Gloria for approval as defined in the assessment.
8. Log off from SAS Enterprise GRC.

Example: Assessment Approver Reviews and Approves the Assessment Completion

Gloria approves the completed assessment. Complete these steps as Gloria:

1. Gloria has received notification via the task list that she needs to approve the completed assessment. Click on the task link, and on the assessment window, review the assessment, and click **Validate**. Enter a change reason, and click **Save**. The assessment is now Closed.

2. Log off from SAS Enterprise GRC.

Implementing a Questionnaire-Based Risk Assessment

Example Questionnaire-Based Assessment Process

The securities department at Orion Star is rolling out their GRC infrastructure, and is implementing a questionnaire-based assessment process to assess risks, causes, and controls. For the purpose of this example, the following table displays the users involved in performing a risk assessment and their job titles and roles. The responsibilities and roles that you define vary depending on your organization.

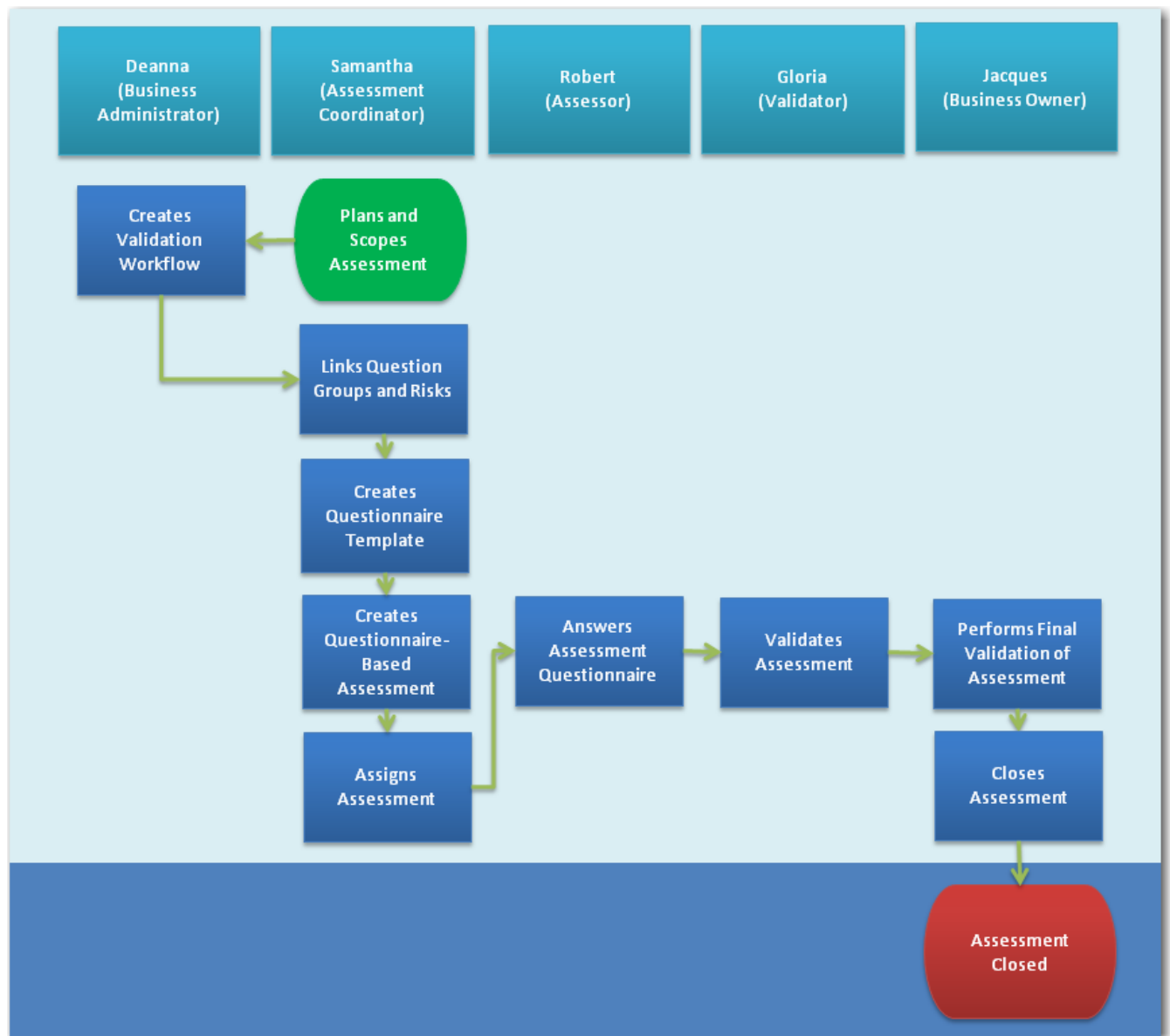
Table 13.6 *Example Assessment Users and Roles*

User	Job Title	SAS Enterprise GRC Roles
Deanna Tiswell	Administrator	Enterprise GRC: Administration
Robert Fitzgerald	Securities Department Risk Manager	Enterprise GRC: Assessment
Samantha Glass	Risk Coordinator	Enterprise GRC: Assessment Coordination
Jacques Simon	Central Operational Risk Manager, Investment Banking	Enterprise GRC: Business Ownership
Gloria Hyatt	Investment Banking Division Expert	Enterprise GRC: Assessment Approval Enterprise GRC: Assessment Questionnaire Approval

In this example, the IT Security group at Orion Star is sending questionnaires to assess the internal fraud risk. The risk is under the purview of the Securities Department. Therefore, Robert has the role of Assessor. Ultimate ownership of assets falls to the Central Risk Manager, Jacques, who is the Business Owner in this example.

The Risk Coordinator, Samantha, is planning to review risks on a quarterly basis. These questionnaire-based assessments are completed by Robert, reviewed by Jacques, and validated by Gloria. This specific example uses a questionnaire-based assessment process.

The following figure describes the business process for the example of Orion Star.

Display 13.3 Example Questionnaire-Based Risk Assessment Business Process for Internal Fraud at Orion Star

The assessment process that follows assumes that the Administrator has already created or imported certain assessment data objects, such as questions. Other objects are already available as part of the sample data. Therefore, no additional steps are required. See “Defining Assessment Data Objects” on page 151 for additional information.

Example Questionnaire-Based Assessment Steps

The questionnaire-based assessment example follows these steps:

1. Deanna, the Administrator, [creates the initial assessment validation workflow](#).
2. Samantha, the Risk Assessment Coordinator, [links a question group to a risk](#).
3. Samantha, the Risk Assessment Coordinator, [creates a new questionnaire template](#).
4. Samantha, the Risk Assessment Coordinator, [creates a new questionnaire-based assessment](#).

5. Robert, the Assessor, [responds to the risk assessment questionnaire](#).
6. Gloria, the Assessment Approver, [validates the questionnaire](#).
7. Jacques, the Central Risk Manager, [fully validates the questionnaire and closes the risk assessment](#).

Example: Administrator Creates the Questionnaire-Based Validation Workflow

Deanna, the Administrator, creates the initial validation workflow. Complete these steps as Deanna:

1. Select **Risk Management > Assessment Validation Workflow** from the menu. The Assessment Validation Workflow window appears.
2. Select the operational area for the scenario. In the OL chooser, click **Edit** and in the Operational Point window, select the following dimension and node from the Dimension drop-down list, and click **Add** for each.
 - Dimension: **Management Organization**
Node: **Management Organizations > iFinance > Investment Banking > Securities**

Click **OK** to add the operational point and return to the previous window.
3. In the Current Validation Stages table, click **Create Validation Stages**. The Edit Validation Stages window appears.
4. Click **Add Validation Stage**. The Add Validation Stage window appears.
5. Enter the name of the first validation stage, *First Validation Stage for Securities Department Assessments*, in the **Name** field.
6. Click **Add User**. The View Users window appears. Select Gloria as the Validator and return to the Add Validation Stage window.
7. Click **OK** to return to the Edit Validation Stages window.
8. Click **Add Validation Stage**. The Add Validation Stage window appears.
9. Enter the name of the second validation stage, *Second Validation Stage for Securities Department Assessments*, in the **Name** field.
10. Click **Add User**. The View Users window appears. Select Jacques as the Validator and return to the Add Validation Stage window.
11. Click **OK** to return to the Edit Validation Stages window.
12. Click **Save**, enter a reason for the change in the Change Reason window, and click **Save** again.
13. Log off from SAS Enterprise GRC.

Example: Risk Assessment Coordinator Links a Risk Event Type to a Question Group

The following example assumes that you have created the example risk and loaded the example question group and associated questions.

To create the example risk, see [“Example Risk Creation Process” on page 153](#).

To load the example question group and questions, see “[Example: Data Loading Questions and Question Groups for a Questionnaire-Based Assessment](#)” on page 201.

Samantha links the risk event type to a question group. Complete these steps as Samantha:

1. Select **Risk Management > Libraries** from the menu. The Libraries window appears.
2. From the left pane of the Libraries window, click **Question Groups**, and click on the internal fraud exposure question group.
3. From the left pane of the question group, click **Assessment Items**, and then click **Add Item**. The Operational Point window appears. Use the OL chooser to select the following dimension and node from the Dimension drop-down list.
 - Dimension: **Risk Event Type**
Node: **Internal Fraud > Unauthorized Activity > Mismarking of position (intentional)**

Click **OK** to add the operational point and return to the previous window.
4. Risks that meet the criteria of this risk event type, such as the one you created, can now be associated with this question group. Click **Save** to save the question group.

Example: Risk Assessment Coordinator Creates a Questionnaire Template

Samantha creates a questionnaire template as Risk Assessment Coordinator. Complete these steps as Samantha:

1. Select **Risk Management > Libraries** from the menu. The Libraries window appears.
2. From the left pane, click **Questionnaire Templates**, and click **Create Questionnaire Template**. The Create Questionnaire Template window opens.
3. Edit the operational area for the questionnaire template. In the OL chooser, click **Edit**. In the Operational Area window, select the following dimensions and nodes from the Dimension drop-down list, and click **Add** for each.
 - Dimension: **Management Organization**
Node: **Management Organizations > iFinance > Investment Banking > Securities**
 - Dimension: **Geography**
Node: **Geographies > Americas > North America > United States**

Click **OK** to add the operational area and return to the previous window.
4. Select **No** for **Do you want to create an assessment from this template now?**
5. On the **Details** tab, complete these steps:
 - a. Select **Yes** for the **Is Active?** field.
 - b. Enter *Internal securities fraud questionnaire* in the **Name** field.
 - c. Enter *Questionnaire on internal securities fraud by mismarking positions* in the **Description** field.
 - d. Keep all other defaults, and click the **Risk Event Types** tab.

6. On the **Risk Event Types** tab, complete these steps:
 - a. Click **Add Risk Event Type** to add a risk event type. The Add Risk Event Type window appears.
 - b. Select the **Mismarking of position (intentional)** risk event type, and click **Add and Close**.
 - c. Keep all other defaults, and click the **Layout** tab.
7. On the **Layout** tab, complete these steps:
 - a. Click **Select Question Groups**. The Question Groups window appears.
 - b. Ensure that the question group that you created, **(Fraud-001) Internal Fraud Exposure Group**, is available and selected. Click **OK** to return to the Layout page.
8. Click **Save** to save the questionnaire template.

Example: Risk Assessment Coordinator Creates a Questionnaire-Based Assessment

Samantha creates a questionnaire-based assessment as Risk Assessment Coordinator. Complete these steps as Samantha:

1. Select **Risk Management > Assessments** from the menu. The Assessments window appears.
2. This assessment is questionnaire-based. Click **Create Assessment**, and select **Questionnaire-Based**. The Create Assessment window appears.
3. Edit the operational area for the questionnaire assessment. In the OL chooser, click **Edit**. In the Operational Area window, select the following dimensions and nodes from the Dimension drop-down list, and click **Add** for each.
 - Dimension: **Management Organization**
Node: **Management Organizations > iFinance > Investment Banking > Securities**
 - Dimension: **Geography**
Node: **Geographies > Americas > North America > United States**

Click **OK** to add the operational area and return to the previous window.
4. On the **Details** tab, complete these steps:
 - a. Enter *Mismarked Position Fraud Assessment* in the **Assessment Name** field.
 - b. Select an appropriate **Assessment Period** from the drop-down list.
 - c. Keep all other defaults, and click the **Questionnaire Template** tab.
5. On the **Questionnaire Template** tab, select *Internal securities fraud questionnaire*. Click the **Positions** tab.
6. On the **Positions** tab, complete these steps:
 - a. Select the check mark next to the Enterprise GRC: Assessment role in the **Positions** table.
 - b. On this row, click the link to the **Selected Risks**. The Select Risks window appears.

- c. On the Select Risks window, select the **Mismarking of position (intentional)** risk from the list of associated risks. Click **Save** to return to the previous window..
- d. Click the **Notify List** tab.
7. On the **Notify List** tab, click **Add**. Select Jacques, and then click the **Summary** tab.
8. On the **Summary** tab, verify that you have selected **Yes** for the **Do you want to open the assessment now?** field. Click **Save**. The Open Assessment window appears.
9. In the Open Assessment window, select the **Enterprise GRC: Assessment** role, and click **Open**. The assessment is sent.
10. Log off from SAS Enterprise GRC.

Example: Assessor Responds to the Risk Assessment Questionnaire

Robert responds to the risk assessment questionnaire as Assessor. Complete these steps as Robert:

1. Robert has received notification via the task list that he needs to complete an assessment. Click on the task link. On the assessment window, click the **Questionnaires** tab, and click on the questionnaire link.
2. Robert believes the risk of direct financial loss is high for an internal fraud exposure that involves the mismarking of positions. He rates it 3.6 on a scale from 1 to 4. Click **Begin Modification**, enter 3.6, and enter a justification.
3. Robert has found the average loss from one of these events is \$34,000. Enter 34000, and enter a justification.
4. Click **Submit** to submit the results to Gloria for validation, click **Done**, and then click **Save**.
5. Log off from SAS Enterprise GRC.


Example: Assessment Validator Reviews and Approves the Questionnaire-Based Assessment

Gloria validates the initial assessment plan as Validator. Complete these steps as Gloria:

1. Select **Risk Management > Assessments** from the menu. Click on the fraud assessment. On the assessment window, click the **Questionnaires** tab, and click on the questionnaire link.
2. Gloria is satisfied with the assessment results. On the assessment window, review the assessment, and click **Validate**.
3. Log off from SAS Enterprise GRC.

Example: Business Owner Fully Validates and Closes the Questionnaire-Based Assessment

Jacques performs final validation for the questionnaire-based assessment as Business Owner, and closes the assessment. Complete these steps as Jacques:

1. Select **Risk Management > Assessments** from the menu. Click on the fraud assessment. On the assessment window, click the **Questionnaires** tab, and click on the questionnaire link.
2. Jacques is satisfied with the assessment results. On the assessment window, review the assessment, and click **Validate**. The assessment is now fully validated. Click **Save** to return to the Assessments window.
3. On the Assessments window, in the Assessments table, click the down arrow icon  next to the validated assessment and select **Close**. The assessment is now closed.
4. Log off from SAS Enterprise GRC.

Chapter 14

Managing Incidents and Incident Workflows

Overview	169
Incidents and Incident Workflows	170
Overview	170
Incident Definitions	171
Roles for Managing Incidents	172
Incident Management Process	173
Incident Investigation – Classification	174
Incident Investigation – Monetary Breakdown	174
Incident Investigation – Issue Thresholds	176
Incident Approval	178
Managing an Example Incident	179
Example Incident and Incident Business Process	179
Example: Administrator Creates the Event Validation Workflow	180
Example: Administrator Creates Additional Validation Workflows	180
Example: Incident Creator Creates an Incident	181
Example: Incident Investigator Completes the Investigation	182
Example: Incident Approver Reviews and Approves the Event	183
Example: Approver Reviews and Approves the Allocations, Financial Effects, and Incident Causes	183

Overview

In SAS Enterprise GRC, *incident management* refers to the process of recording events related to risks, policy violations, and audit items. It also refers to the process of accounting for outcomes associated with these events, such as financial effects (losses), nonfinancial effects, direct recoveries, insurance recoveries, allocations, causes, and failed controls.

This chapter is primarily intended for users who participate in the process of capturing, investigating, auditing, and entering data related to incidents by means of the graphical user interface. For more information about the roles that participate in the incident management process, see [“Roles for Managing Incidents” on page 172](#).

This chapter uses the example of Orion Star, a bank that is using SAS Enterprise GRC to manage its GRC activities. Orion Star wants to use an incident management process to collect information about events that occur within its organization. The example uses the default SAS Enterprise GRC user interface environment. It assumes that you have completed steps in previous chapters to implement the business structure, assign users to

roles, and so on. It also assumes that you understand the workflows that are used for managing incidents.

For more information about this example, see [Chapter 3, “Gathering Governance, Risk, and Compliance Data,”](#) on page 27.

Incidents and Incident Workflows

Overview

SAS Enterprise GRC enables the process of managing incidents and incident-related workflows through the **Incidents** menu. This menu enables you to perform the following tasks:

- Manage incidents through the **Incidents** submenu.
You must have Incident/Event role capabilities assigned to manage the **Incidents** submenu.
- Manage financial effects through the **Financial Effects** submenu. A financial effect is a loss, gain, or a near miss. A financial effect can exist on its own without being linked to an incident, as long as the appropriate access rights are defined. However, a financial effect cannot be linked to more than one incident. An incident can contain multiple financial effects.
You must have Financial Effect role capabilities assigned to manage the **Financial Effects** submenu.
- Manage direct recoveries through the **Direct Recoveries** submenu. Recoveries, which reduce the loss for a specific incident, can occur directly or through insurance. Direct recoveries are the non-insurance portion of a recovery. A direct recovery can exist on its own without being linked to an incident, as long as the appropriate access rights are defined. However, a direct recovery cannot be linked to more than one incident. An incident can contain multiple direct recoveries.
You must have Recovery role capabilities assigned to manage the **Direct Recoveries** submenu.
- Manage insurance recoveries through the **Insurance Recoveries** submenu. Insurance recoveries can reduce losses for an incident. For example, this can occur when an asset is covered through an insurance policy. An insurance recovery can exist on its own without being linked to an incident, as long as the appropriate access rights are defined. However, an insurance recovery cannot be linked to more than one incident. An incident can contain multiple insurance recoveries.
You must have Recovery role capabilities to manage the **Insurance Recoveries** submenu.
- Manage the event validation process through the **Event Validation Workflow** submenu. You can use this area to create and modify the validation process used for events.
You must have the Update capability for the Validation Workflow category that is assigned to a role to manage the **Event Validation Workflow** submenu.
- Manage the financial effect validation process through the **Financial Effect Validation Workflow** submenu. You can use this area to create and modify the validation process used for financial effects.

You must have the Update capability for the Validation Workflow category that is assigned to a role to manage the **Financial Effect Validation Workflow** submenu.

- Manage the allocation validation process through the **Allocation Validation Workflow** submenu. An allocation is used to allocate either the total financial effect, or the net financial effect after recoveries, to different operational areas. An allocation exists only within an incident. An incident can contain multiple allocations. You can use this area to create and modify the validation process used for allocations.

You must have the Update capability for the Validation Workflow category that is assigned to a role to manage the **Allocation Validation Workflow** submenu.

- Manage the recovery validation process through the **Recovery Validation Workflow** submenu. You can use this area to create and modify the validation process used for recoveries.

You must have the Update capability for the Validation Workflow category that is assigned to a role to manage the **Recovery Validation Workflow** submenu.

- Manage the cause validation process through the **Cause Validation Workflow** submenu. A cause is something that contributed to the occurrence of the incident. You can use this area to create and modify the validation process used for causes.

You must have the Update capability for the Validation Workflow category that is assigned to a role to manage the **Cause Validation Workflow** submenu.

- Manage issues thresholds through the **Issue Thresholds** submenu. Issue thresholds are ranges in which a financial effect creates an issue.

You must have Threshold Definition role capabilities assigned to manage the **Issue Threshold** submenu.

For more information about issue thresholds, see [Issue Thresholds on page 176](#).

Incident Definitions

An incident can contain the following objects as defined below:

event

An event is used to record basic information about the incident. An incident always contains exactly one event.

financial effect

A financial effect is a loss, gain, or a near miss. A financial effect can exist on its own without being linked to an incident, as long as the appropriate access rights are defined. However, a financial effect cannot be linked to more than one incident. An incident can contain multiple financial effects.

effect amount

An effect amount is used to record individual amounts that are associated with a financial effect. An effect amount exists only within a financial effect. A financial effect can contain multiple effect amounts.

nonfinancial effect

A nonfinancial effect records the nonfinancial effects, such as negative media coverage, of an incident. A nonfinancial effect exists only within an incident. An incident can contain multiple nonfinancial impacts.

recovery

A recovery can be a direct recovery or an insurance recovery that reduces the impact of a loss. A recovery can exist on its own without being linked to an incident, as long

as the appropriate access rights are defined. However, a recovery cannot be linked to more than one incident. An incident can contain multiple recoveries.

recovery amount

A recovery amount is used to record individual amounts that are associated with a direct recovery or an insurance recovery. A recovery amount exists only within a direct recovery or an insurance recovery. Both types of recoveries can contain multiple recovery amounts.

allocation

An allocation is used to allocate either the total financial effect, or the net financial effect after recoveries, to different operational areas. An allocation exists only within an incident. An incident can contain multiple allocations.

incident cause

An incident cause records the cause or causes that contributed to the occurrence of the incident. If a cause is required by the system for validation (by default a cause is required but this is configurable), an incident must have at least one cause (assigned as 100%) before an incident can be sent for validation.

incident failed control

An incident failed control records the control instance or control instances that failed in the incident. An incident can have multiple failed controls.

effect cause

An effect cause is the same as an incident cause except that it is assigned to a financial effect instead of an incident. Unlike incident causes, you do not have to assign a full percentage (100%) to an effect cause to send an incident for validation.

effect failed control

An effect failed control is the same as an incident failed control except that it is assigned to a financial effect instead of an incident.

The following incident-related objects can be validated: events, financial effects, allocations, recoveries, and incident causes. (Effect causes cannot be validated.)

No history is available for nonfinancial effects, causes, failed controls, or allocations. The history of these objects is maintained by the parent object. For example, the history of an effect cause is maintained by the corresponding financial effect. Also, when a financial effect, direct recovery, or insurance recovery is linked to an incident, the history of these objects is also maintained by the incident.

Roles for Managing Incidents

Capabilities to manage incidents are assigned through roles. The following table describes each role as it pertains to incident management.

Table 14.1 Roles for Incident Management

Role	Description
Enterprise GRC: Administration	Administrator. Administers the SAS Enterprise GRC environment. Might have responsibilities for maintaining incident workflows and issue thresholds.
Enterprise GRC: Incident Creation	Incident Creator. Responsible for creating and submitting incidents.

Role	Description
Enterprise GRC: Incident Investigation	Incident Investigator. Responsible for investigating incidents.
Enterprise GRC: Incident Risk Approval	Incident Approver. Responsible for reviewing and approving incident investigations at the risk and management level.
Enterprise GRC: Incident Management Approval	
Enterprise GRC: Allocation Risk Approval	Allocation, Recovery, and Financial Effect Approver. Reviews and approves allocations, recoveries, and financial effects. Approval stages can occur at the risk and management level.
Enterprise GRC: Allocation Management Approval	
Enterprise GRC: Recovery Risk Approval	
Enterprise GRC: Recovery Management Approval	
Enterprise GRC: Financial Effect Risk Approval	
Enterprise GRC: Financial Effect Management Approval	
Enterprise GRC: Incident Cause Risk Approval	Cause Approver. Reviews and approves incident causes at the risk and management level.
Enterprise GRC: Incident Cause Management Approval	

Incident Management Process

The incident management process is completed using the following steps:

1. The Administrator works with the Risk Manager to initially define the following in SAS Enterprise GRC:
 - event validation workflows
 - financial effect validation workflows
 - allocation validation workflows
 - recovery validation workflows
 - cause validation workflows
 - issue thresholds
2. The Incident Creator discovers an event has occurred and creates an incident.
3. Incident Investigators accept the incident, investigate the incident, and provide details about the following items:
 - financial and nonfinancial effects
 - recoveries
 - allocations

- causes
- failed controls

One or more investigators can be involved in this stage to capture the required data. After all information has been gathered by all parties, the incident is sent for approval.

4. Approvers review and approve the incident. One or more approvers can be involved in this stage. The approval process repeats until the responses have been verified at all workflow stages. After all required approvers have approved the incident details, the incident is fully approved.

Incident Investigation – Classification

The overall classification of an incident is calculated on the Event page of the Investigate Incident window. This classification, which is measured on an ordinal scale, is the maximum of the financial effects classification and the nonfinancial effects classification. The ordinal scale is defined by the administrator. For more information about defining classifications, see the *SAS Enterprise GRC: Administration and Customization Guide*.

For example, the ordinal scale might have the following four levels: none, low, medium, and high. This scale is used throughout the rest of this section. The same ordinal scale is used for overall classification, financial effects classification, and nonfinancial effects classification. Of the three classifications, only the overall classification is displayed.

The classification for nonfinancial effects is determined by the maximum classification across all nonfinancial effects. For example, if you have two medium nonfinancial effects and one low nonfinancial effect, then the nonfinancial effects classification is medium.

The classification for financial effects is determined by the **Total Booked Amount** value and the threshold values that have been defined by the administrator. The number of threshold values should be one less than the number of levels on the ordinal scale.

Incident Investigation – Monetary Breakdown

During the investigation phase of an incident, SAS Enterprise GRC provides a monetary breakdown of losses and recoveries. The monetary breakdown table contains the following items. All amounts are displayed in the base currency. Negative amounts are indicated by the word "Loss" in the first column rather than by a negative sign.

Gross

The Gross field is calculated by summarizing across all financial effects and the corresponding effect amounts. Amounts that correspond to a Gain effect nature are added. Amounts that correspond to Loss or Gain effect natures are subtracted. An effect amount is included in the summarization only if it satisfies the following two conditions:

- The effect amount status must be Settled, Cost, or Provisioned.
- The effect type must correspond to the following effect type attribute: Include in Gross Calculation. Effect amounts that correspond to the Exclude from Gross Calculation effect type attribute are not included in the summarization.

If the resulting number is positive, then the number is reported as Gross Gain. If the resulting number is negative, then the number is reported as Gross Loss.

Direct Recoveries

The Direct Recoveries field is calculated by summing all settled direct recovery amounts across all direct recoveries.

Net Before Insurance Recoveries

This field is calculated by summing Gross and Direct Recoveries. If the resulting number is positive, then the number is reported as Net Gain Before Insurance Recoveries. If the resulting number is negative, then the number is reported as Net Loss Before Insurance Recoveries.

Insurance Recoveries

The Insurance Recoveries field is calculated by summing all settled insurance recovery amounts across all insurance recoveries.

Total Recoveries

This field is calculated by summing Direct Recoveries and Insurance Recoveries.

Net

The Net field is calculated by summing gross and total recoveries. If the resulting number is positive, then the number is reported as Net Gain. If the resulting number is negative, then the number is reported as Net Loss.

Suppose that you are investigating an incident that has a financial effect, a direct recovery, and an insurance recovery. The financial effect has a Loss effect nature and two settled effect amounts of EUR 3,000 and EUR 4,000. Each effect amount corresponds to an effect type that is included in the gross calculation. The direct recovery has a EUR 6,000 recovery amount, and the insurance recovery has a EUR 4,000 recovery amount. The resulting monetary breakdown is shown in the following figure.

Display 14.1 Example Monetary Breakdown

Monetary Breakdown	Currency	Amount	Amount (EUR)
Gross Loss	EUR	7,000	7,000
Direct Recoveries	EUR	6,000	6,000
Net Loss Before Insurance Recoveries	EUR	1,000	1,000
Insurance Recoveries	EUR	4,000	4,000
Total Recoveries	EUR	10,000	10,000
Net Gain	EUR	3,000	3,000

The Gross is EUR -7,000, which is the result of summing the two individual loss effect amounts. Because this result is negative, the field is labeled Gross Loss.

The Net Before Insurance Recoveries is EUR -1,000 = -7,000 + 6,000. Because the result is negative, the field is labeled Net Loss Before Insurance Recoveries.

The Total Recoveries amount is EUR 10,000 = 6,000 + 4,000.

The Net is EUR 3,000 = -7,000 + 10,000. Because the result is positive, the field is labeled Net Gain.

Incident Investigation – Issue Thresholds

Overview of Issue Thresholds

During the investigation phase of an incident, SAS Enterprise GRC tracks the incident to determine whether a predefined *issue threshold* is breached. SAS Enterprise GRC automatically creates issues whenever the financial effects within an incident breach the threshold and status of the incident changes to Approved. Issues thresholds can apply to any combination of the following incident types:

- losses
- gains
- near misses

Issue thresholds work in the following way. For example, in SAS Enterprise GRC, you define the following range values:

Table 14.2 Issue Thresholds

Lower Range	Upper Range	Issue Priority
0	5000	Low
5000	10000	Medium
10000	20000	High
20000	250000	Critical

The value x represents a value in the range.

Low priority	$x \geq 0$ and $x < 5000$
Medium priority	$x \geq 5000$ and $x < 10000$
High priority	$x \geq 10000$ and $x < 20000$
Critical priority	$x \geq 20000$ and $x \leq 250000$

No issues are created for values outside the scope of this range. You can leave the maximum threshold value blank to specify that there is no maximum limit.

The **Total Booked Amount** value from the Effects page of the Investigate Incident window is used to determine whether an issue threshold is breached.

In order for a breach to be determined, an issue threshold must have certain attributes in common with an incident. First, the issue threshold must be defined so that it applies to the same incident type. For example, if an issue threshold applies only to near misses, then a breach is not determined if the incident type is **Loss/Profit**. Second, the domain of the issue threshold must contain the entire domain of the incident. For example, if an incident is defined at Management Organization > iFinance and Geography > Americas, then the issue threshold must be defined at either Management Organization > iFinance or Geography > Americas. Issue thresholds that are defined at a particular node also apply to all children nodes. For example, if an issue threshold is defined at Management Organization > iFinance, then the threshold also applies to incidents defined at Management Organization > iFinance > Retail Banking.

It is possible for a single incident to breach several thresholds at once. In this situation, the breached threshold value that is reported in the created issue depends on the most specific operational location. Thus, if different threshold values existed at Management Organization > iFinance and Management Organization > iFinance > Retail Banking, the issue would use the value that was breached in the Management Organization > iFinance > Retail Banking operational location. If two threshold breaches occur at the same operational location, then the lowest minimum value is used.

When an incident first breaches an issue threshold, the investigator of the incident is notified via a message that is displayed at the top of the Effects page.

When an incident that has breached an issue threshold is Approved without Quality Review or Approved Pending a Quality Review, the owner of the incident is notified by e-mail and by the task list under the label Issues Being Drafted. In addition, an issue is automatically created. The issue contains the following data:

- Domain. This is the same as the Event Domain of the incident.
- Title. This is the same as the title of the incident.
- Issue ID. This is system generated.
- Priority. This is inherited from the Issue Priority of the issue threshold.
- Owner. This is the same as the investigator of the incident.
- Originator. This is the same as the investigator of the incident.
- Date Created. This is the date that SAS Enterprise GRC automatically creates the issue.
- Linked Items. This is a hyperlink to the originating incident.
- Source Module. This is populated as Incident Management.

Example Issue Threshold

Suppose that you want to create a high priority issue whenever a near-miss incident occurs in the United States that exceeds 10,000. The issue threshold used to perform this task is shown in the following figure.

Display 14.2 Example Issue Threshold

* Event Domain

[Edit](#) | [Clear](#) | [Favorites](#)

Risk Event Type:

(None Selected)

Management Organization:

(None Selected)

Geography:

Americas > North America > United States

Product:

(None Selected)

Process:

(None Selected)

* Applies To:

☐ Losses
 ☐ Gains
 ☒ Near Misses

* Minimum Threshold:

10,000

Maximum Threshold:


* Issue Priority:

High



Suppose that you now create a near-miss incident that has two financial effects with effect amounts of EUR 6,000 and EUR 5,000. The total of these financial effects exceeds the threshold of EUR 10,000. Therefore, an issue with priority **High** is created. This fact is indicated in the following figure.

Display 14.3 Example: Exceeding an Issue Threshold

Effects


Information
×

The issue threshold value for this incident has been exceeded. An issue will be opened for this incident.

Financial Effects		Create Financial Effect... Link...		
	Amount	Currency	Effect Nature (Financial Effect)	Remove
1	6,000.00	EUR	Near Miss	
2	5,000.00	EUR	Near Miss	

Rows 1 to 2 of 2

Total Financial Effects (Near Miss): EUR 11,000.00

Incident Approval

The approval of incidents is unique among the objects in SAS Enterprise GRC in several ways:

- Objects within an incident can be sent for approval at different times and are approved independently of each other. The event, financial effects, recoveries, incident causes, and allocations all have an independent approval process.
- Each object that can be approved has two validation phases by default: Management Approval and Risk Approval. For each object, any applicable management validation workflow stages must complete before the risk approval phase can begin.
- You can create validation workflows for each object by adding validation stages in the user interface or by adding validation stages to the incident management workflow template. By default, the product uses the SAS Workflow Studio incident management workflow but incorporates any validation stages that you have added in the user interface. You can also turn the SAS Workflow Studio incident management workflow off entirely. For more information about the incident management workflow, see “The Default Incident Management Workflow” in the *SAS Enterprise GRC: Workflow Administration Guide*.

It is possible for different objects within the same incident to be in different phases. For example, an allocation can go through risk approval and already be in management approval before a financial effect is even sent for management approval.

The approval process ends when all objects with the incident have been approved in both the management phase and the risk phase.

Managing an Example Incident

Example Incident and Incident Business Process

The securities department at Orion Star is using SAS Enterprise GRC to manage incidents, and has discovered internal fraud has occurred. A rogue trader has used insider information to make trades on securities. Orion Star is still in the process of investigating, but an initial estimate is that the fraud will cost the company \$200,000. For the purpose of this example, the following table displays the users involved in controls and testing and their job titles and roles. The responsibilities and roles that you define vary depending on your organization.

Table 14.3 Example Incident Users and Roles

User	Job Title	SAS Enterprise GRC Roles
Deanna Tiswell	Administrator	Enterprise GRC: Administration
Robert Fitzgerald	Securities Department Risk Manager	Enterprise GRC: Incident Management Validation
Wendy Feinstein	Securities Department Investigator	Enterprise GRC: Incident Investigation
Gloria Hyatt	Investment Banking Division Expert	Enterprise GRC: Allocation Management Approval Enterprise GRC: Financial Effect Management Approval Enterprise GRC: Recovery Management Approval Enterprise GRC: Incident Cause Management Approval
Victor Osgoode	Securities Department Team Lead	Enterprise GRC: Incident Creation

Victor, a trader within the securities group, is creating an incident and assigning Wendy, the department auditor, to investigate.

The incident is fully investigated by Wendy and then approved by Gloria and Robert, who are assigned to validate all aspects of the incident. Robert approves the Event. Gloria assumes the multiple roles of Financial Effect, Allocation, and Cause Approver. Because there was no recovery involved in this example, her role as Recovery Approver does not apply.

The example follows these steps:

1. Deanna, the Administrator, [creates the event validation workflow](#).
2. Deanna, the Administrator, [creates the other validation workflows](#).

3. Victor **creates a new incident** as Incident Creator.
4. Wendy **investigates the incident** as Incident Investigator.
5. Robert **approves the event** as Incident Approver.
6. Gloria **approves the allocations, financial effects, and incident causes**.

Example: Administrator Creates the Event Validation Workflow

Deanna, the Administrator, creates the event validation workflow for Robert. Complete these steps as Deanna:

1. Select **Incidents > Event Validation Workflow** from the menu. The Event Validation Workflow window appears.
2. Select the operational area for the control. In the OL chooser, click **Edit** and in the Operational Point window, select the following dimensions and nodes from the Dimension drop-down list and click **Add** for each.
 - Dimension: **Management Organization**
Node: **Management Organizations > iFinance > Investment Banking > Securities**
 - Dimension: **Geography**
Node: **Geographies > Americas > North America > United States**

Click **OK** to add the operational point and return to the previous window.
3. In the Current Validation Stages table, click **Create Validation Stages**. The Edit Validation Stages window appears.
4. The incident goes through management approval. Click **Add Management Validation Stage**. The Add Validation Stage window appears.
5. Enter the name of the validation stage, *Approval Stage for Securities Department*, in the **Name** field.
6. Click **Add User**. The Select a User window appears. Select Robert as the Validator and return to the Add Validation Stage window.
7. Click **OK** to return to the Edit Validation Stages window.
8. This validation does not require multiple validation stages. Click **Save**, enter a reason for the change in the Change Reason window, and click **Save** again.

Example: Administrator Creates Additional Validation Workflows

Deanna, the Administrator, creates the other validation workflows for Gloria. Complete these steps as Deanna:

1. Select **Incidents > Financial Effect Validation Workflow** from the menu. The Financial Effect Validation Workflow window appears.
2. Select the operational area for the control. In the OL chooser, click **Edit**. In the Operational Point window, select the following dimensions and nodes from the Dimension drop-down list and click **Add** for each.
 - Dimension: **Management Organization**

Node: **Management Organizations > iFinance > Investment Banking > Securities**

- Dimension: **Geography**

Node: **Geographies > Americas > North America > United States**

Click **OK** to add the operational point and return to the previous window.

3. In the Current Validation Stages table, click **Create Validation Stages**. The Edit Validation Stages window appears.
4. Click **Add Management Validation Stage**. The Add Management Validation Stage window appears.
5. Enter the name of the validation stage, *Approval Stage for Securities Department*, in the **Name** field.
6. Click **Add User**. The Select a User window appears. Select Gloria as the Validator and return to the Add Validation Stage window.
7. Click **OK** to return to the Edit Validation Stages window.
8. This validation does not require multiple validation stages. Click **Save**, enter a reason for the change in the Change Reason window, and click **Save** again.
9. Repeat these workflow creation steps for the following validation workflows:
 - **Allocation Validation Workflow**
 - **Cause Validation Workflow**
10. Log off from SAS Enterprise GRC.

Example: Incident Creator Creates an Incident

Victor creates a new incident as Incident Creator. Complete these steps as Victor:

1. Select **Incidents > Incidents** from the menu. The Incidents window appears.
2. Click **Create Incident**. The Create Incident window appears.
3. Edit the operational area for the control. In the OL chooser, click **Edit**. In the Operational Area window, select the following dimensions and nodes from the Dimension drop-down list and click **Add** for each.
 - Dimension: **Management Organization**
Node: **Management Organizations > iFinance > Investment Banking > Securities**
 - Dimension: **Geography**
Node: **Geographies > Americas > North America > United States**

Click **OK** to add the operational area and return to the previous window.
4. In the **Event Type** drop-down list, select **Loss/Profit**.
5. Enter *Internal Fraud* in the **Summary Description** field.
6. Leave the default dates in the **Discovery Date**, **Start Date**, and **End Date** fields.
7. Enter *200000* in the **Estimated Amount** and select **USD** from the currency drop-down list.

8. Keep all other defaults, and click **Submit for Investigation**. The incident is queued for incident investigators to complete.
9. Log off from SAS Enterprise GRC.

Example: Incident Investigator Completes the Investigation

Wendy investigates the incident as Incident Investigator. Complete these steps as Wendy:

1. Wendy has received notification via the task list that she needs to accept the incident for investigation. Click on the task link, and on the View Incident window, review the incident, and click **Accept**. The Event page opens.
2. In the Event Operational Point area, click **Edit** to open the OL chooser. In the Operational Area window, select the following additional dimensions and nodes from the Dimension drop-down list and click **Add** for each.

- Dimension: **Risk Event Type**

Node: **Internal Risk Event Types > Internal Fraud > Theft and Fraud > Insider Trading**

- Dimension: **Product**

Node: **Products > Securities**

Click **OK** to add the operational area and return to the previous window.

3. In the **Incident Title** field, enter *Insider Trading*.
4. In the **Event Description** field, enter *Employees used insider information on investment banking deal to trade securities*.
5. During the fraud investigation, the Securities and Exchange Commission was notified and the employee was terminated. In the **Steps Taken** field, enter *SEC notified, parties involved terminated*.
6. Click on **Effects** in the left pane of the window. The Effects page opens.
In the Financial Effects table, click **Create Financial Effect**. The Create Financial Effect window appears.
7. In the Operational Point area, click **Edit** to open the OL chooser. In the Operational Area window, select the following additional dimensions and nodes from the Dimension drop-down list, and click **Add** for each.
• Dimension: **Business Line**
Node: **Internal Business Lines > iFinance > Investment Banking > Securities**
Click **OK** to add the operational area and return to the previous window.
8. The financial effect in this instance was an SEC fine that caused a loss of \$220,000. In the **Effect Title** field, enter *SEC fine*.
9. In the **Effect Description** field, enter *SEC fined company for \$220,000*.
10. In the Effect Amounts table, click **Create Effect Amount**. The Create Effect Amount window appears.
11. In the **Title** field, enter *SEC fine*.
12. In the **Description** field, enter *SEC fine of \$220,000*.
13. In the **Effect Type** field, select **Regulatory**.

14. In the **Date of Booking**, select an appropriate date.
15. In the **Effect Amount**, enter 220000 and select **USD** for the currency.
16. In the **Effect Amount Status**, select **Settled**. Keep all other defaults, and click **Save** to return to the previous window. Then click **OK** to return to the Effects window.
17. There were no recoveries in this example. Click **Allocations** in the left pane of the window to allocate losses. The Allocations page opens. In the Allocations table, select the option to allocate by **Percentage**, and then click **Allocate**. The Allocate window appears.
18. Details of the accounting transaction are recorded here. In the **Percentage** field, enter 100.
19. In the **Account Number** and **Posting Number** fields, enter the account number and posting number to which this loss is allocated (for example, 12345 and 1001, respectively).
20. Select an accounting book from the **Accounting Book** drop-down list.
21. In the **Allocation Description** field, enter *Allocated to Securities Group*. Keep all other defaults, and click **OK** to return to the previous window.
22. Click **Causes** from the left pane of the window. The Causes page opens. In the Incident Causes table, click **Select Cause**. The Select Cause window appears.
23. Wendy has determined that the cause for the fraud was not a failure on the part of systems or processes, but people. In the **Cause Type**, select the node under **People** > **Lack of integrity of people**.
24. In this example, this was the only reason for the loss. In the **Cause Weight**, enter 100. Click **OK** to return to the previous window.
25. Click **Choose Next Action**, and then review the incident components. For each incident component, select **Send for Approval**. Click **OK**, enter a **Change Reason**, and click **Save** to send the incident components to Robert and Gloria for approval.
26. Log off from SAS Enterprise GRC.

Example: Incident Approver Reviews and Approves the Event

Robert approves the event as Incident Approver. Complete these steps as Robert:

1. Robert has received notification via the task list that he needs to approve an incident. Click on the task link, and in the incident window, review the event.
2. Click **Choose Next Action**, review the incident component, select **Approve** for the **Next Action**, and then click **OK**. Enter a **Change Reason**, and click **Save** to approve the incident.
3. Log off from SAS Enterprise GRC.

Example: Approver Reviews and Approves the Allocations, Financial Effects, and Incident Causes

Gloria validates the allocation, financial effects, and incident cause as Approver. Complete these steps as Gloria:

1. Gloria has received notification via the task list that she needs to complete approvals on allocations, financial effects, and incident causes. Click on the task link, and in the incident window, review the allocations, financial effects, and cause of incident.
2. Click **Choose Next Action**, review the incident components, select **Approve** for the **Next Action** for each component, and then click **OK**. Enter a **Change Reason**, and click **Save** to approve the incident. The incident is now Fully Approved.
3. Log off from SAS Enterprise GRC.

Note: The order is interchangeable for completing the approval steps in this example.

Chapter 15

Viewing Reports






Overview of Reports	185
Example: Running a Stored Process Report	188
Example: Creating a Report Using an Information Map in SAS Web Report Studio	189
Example: Launching a SAS Business Intelligence Dashboard	193

Overview of Reports

Risk managers, executives, and other governance, risk, and compliance experts should regularly review the risk status of the organization and make decisions that continually improve GRC operations.

The **Reports** menu in SAS Enterprise GRC enables you to run, view, and export reports. You can then use the output for decision making.

There are five types of reports:

- SAS Stored Process reports ()
- SAS Information Maps ()
- SAS Web Report Studio reports ()
- SAS BI Dashboards ()
- SAS Visual Analytics Designer ()

The following folders are provided by default for categorizing and storing reports:

- Audit Management
- Compliance
- Control Testing
- Governance
- Incident Management

- Issue and Action Plan
- KRI
- OpRisk Global Data
- Policy Management
- Risk Management
- Sample
- Scenario

Nine folders contain default report stored processes for generating reports: Audit Management, Control Testing, Incident Management, Issue and Action Plan, KRI, OpRisk Global Data, Policy Management, Risk Management, and Sample.

The following table displays the default reports that are available under each report folder:


Table 15.1 Default Report Folders, Reports, and Report Types

Report Folder	Reports Available by Default	Report Type	Description
Audit Management	audit_map	Information Map	Opens an information map for creating audit-related reports.
Control Testing	Certification Progress	Stored Process	Displays a pie chart of controls grouped by certification progress.
	Testing Progress	Stored Process	Displays a pie chart of controls grouped by test status.
	Testing Results	Stored Process	Displays a bar chart of test instances grouped by test results.
	Testing Status	Stored Process	Displays a bar chart of test instances grouped by test status.
Incident Management	event_map	Information Map	Opens an information map for creating incident-related reports.
	Financial Effects Matrix	Stored Process	Displays the number of losses within the selected dimensional point along with the total, minimum, maximum, average loss amount, and the standard deviation.
Issue and Action Plan	actionplan_map	Information Map	Opens an information map for creating action plan related reports.
	issue_map	Information Map	Opens an information map for creating issue-related reports.

Report Folder	Reports Available by Default	Report Type	Description
KRI	Key Risk Indicators	Stored Process	Displays indicators by name and value beside an illustrative gauge graphic.
	kri_map	Information Map	Opens an information map for creating KRI-related reports.
OpRisk Global Data	Operational Risk Matrix	Visual Analytics	Opens the SAS Visual Analytics Designer for creating reports detailing the number of loss events, total loss amount, maximum loss amount, lowest loss amount, and highest loss amount by event risk category and Basel business lines.
Policy Management	policy_map	Information Map	Opens an information map for creating policy-related reports.
Risk Management	Risk Heat Map	Stored Process	Displays a crosstabular report of frequency versus severity ranges.
	risk_indicator_dashboard.dcx	BI Dashboard	Displays a risk indicators dashboard.
	cause_map	Information Map	Opens an information map for creating cause reports that are related to risk assessments.
	control_map	Information Map	Opens an information map for creating control reports that are related to risk assessments.
	risk_indicator_map	Information Map	Opens an information map for creating risk indicator reports.
	risk_map	Information Map	Opens an information map for creating risk reports that are related to risk assessments.
	Risk Summary Dashboard	Visual Analytics	Opens the SAS Visual Analytics Designer for viewing a risk summary dashboard, which is an executive level report that shows the overall health of the SAS Enterprise GRC system. The report contains a risk heat map report, loss event trend report, top 10 KRIs, and a control effectiveness report.
Sample	Test Custom Report	Stored Process	Contains a Test Custom report that shows you how to create a custom report within a custom reporting category. This Test Custom report can be used by administrators to help create and debug customized reports. Because this report is generally useful only while customized reports are being written, the report might be deleted by the administrator.

SAS Enterprise GRC is highly flexible in enabling your organization to customize folders and reports. Any custom reports that have been defined and loaded are also displayed. For information about creating customized folders and reports, see "SAS Enterprise GRC Reporting" in the *SAS Enterprise GRC: Administration and Customization Guide*.

You can take the following actions:

- To search for a particular report-related object, enter the name of the object and click **Search**.
- To open a report folder and view available report-related objects, click on the report folder.
- To navigate up in the folder list, click the navigate-up folder icon () or select a folder from the **Location** drop-down menu.
- To run a stored process report within a folder, click the name of the stored process. The report wizard opens.
- To view a report in SAS Web Report Studio, click the name of the generated report from the folder.
- To view a dashboard in SAS BI Dashboard, click the name of the dashboard from the folder.
- To open an information map in SAS Web Report Studio, click the name of the information map in the folder.
- To open a SAS Visual Analytics Designer report in SAS Visual Analytics, click the name of the report in the folder.
- To save the report as a PDF file, click **Save as PDF** after you have viewed that report. Click **Save** to save the PDF version of the report. To export a report to RTF, click **Export to RTF**. To open an RTF report, click **Open**, and click **Save** to save the RTF version of the report. Click **Cancel** to return to the **Reports** tab.

Example: Running a Stored Process Report

This example demonstrates how to run the Financial Effects Matrix stored process report. This report displays the number of losses within the selected dimensional point along with the total, minimum, maximum, average loss amount, and the standard deviation.

To run the Financial Effects Matrix report:

1. Navigate to the **Incident Management** reports folder.
2. Click **Financial Effects Matrix** to open the report wizard.
3. To filter the report, select an operational location. For information about operational locations, see [“Operational Location and Domain Overview” on page 16](#).
4. Click **Run**.

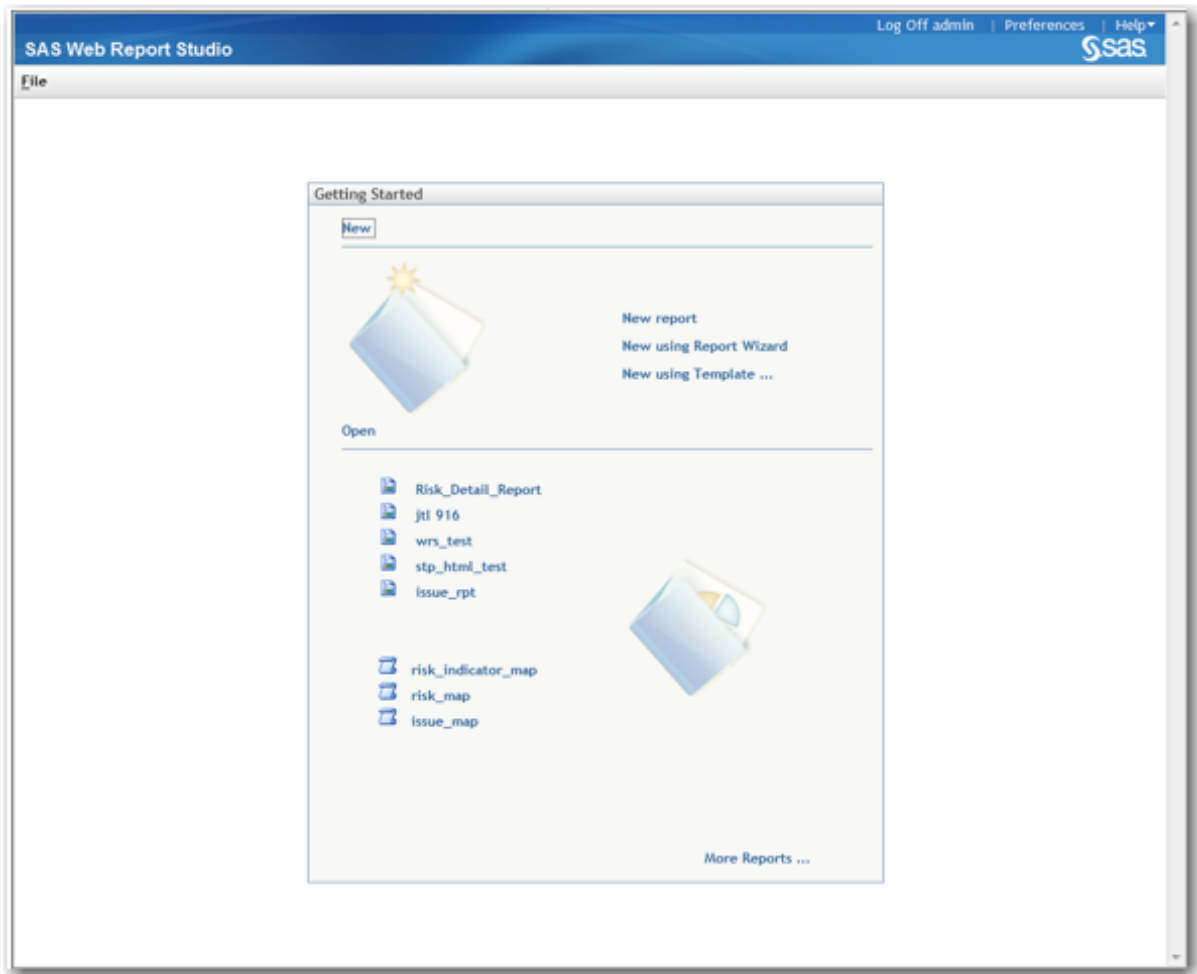
To view a list of the financial effects that are included in the aggregate loss amount, you can click that amount. To view the details of a financial effect, click the ID of that financial effect. The **Edit Financial Effect** window appears.

Example: Creating a Report Using an Information Map in SAS Web Report Studio

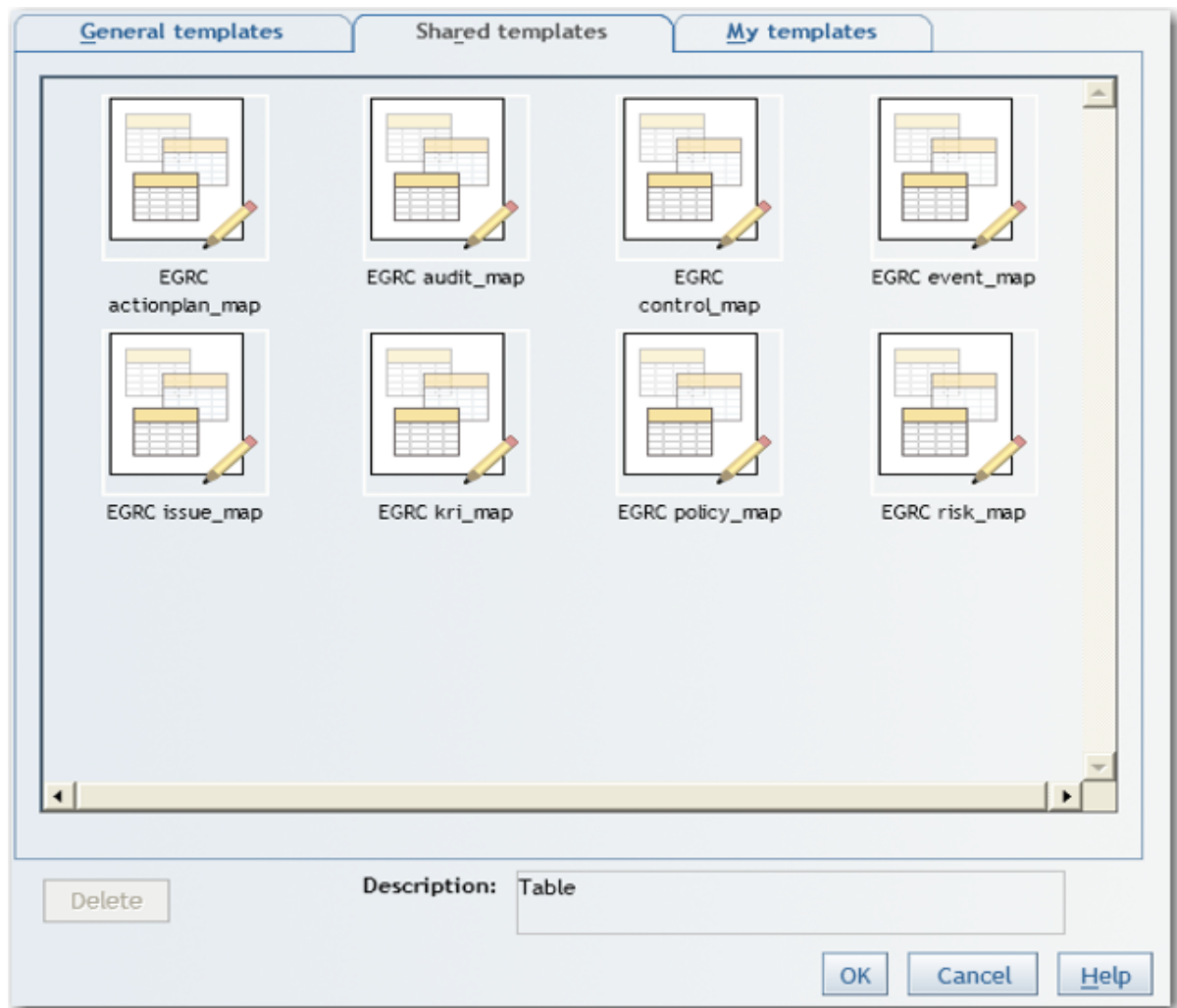
You can use information maps to create SAS Web Report Studio reports.

To create a report using the risk_map information map:

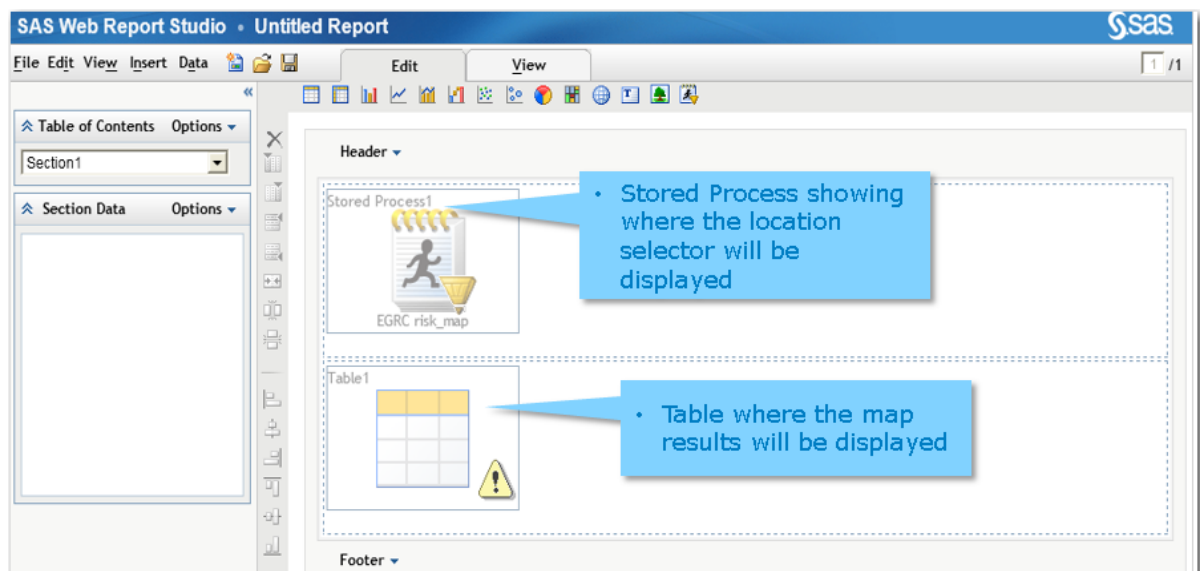
1. Launch SAS Web Report Studio (for example, <http://<server>:<port>/SASWebReportStudio>).



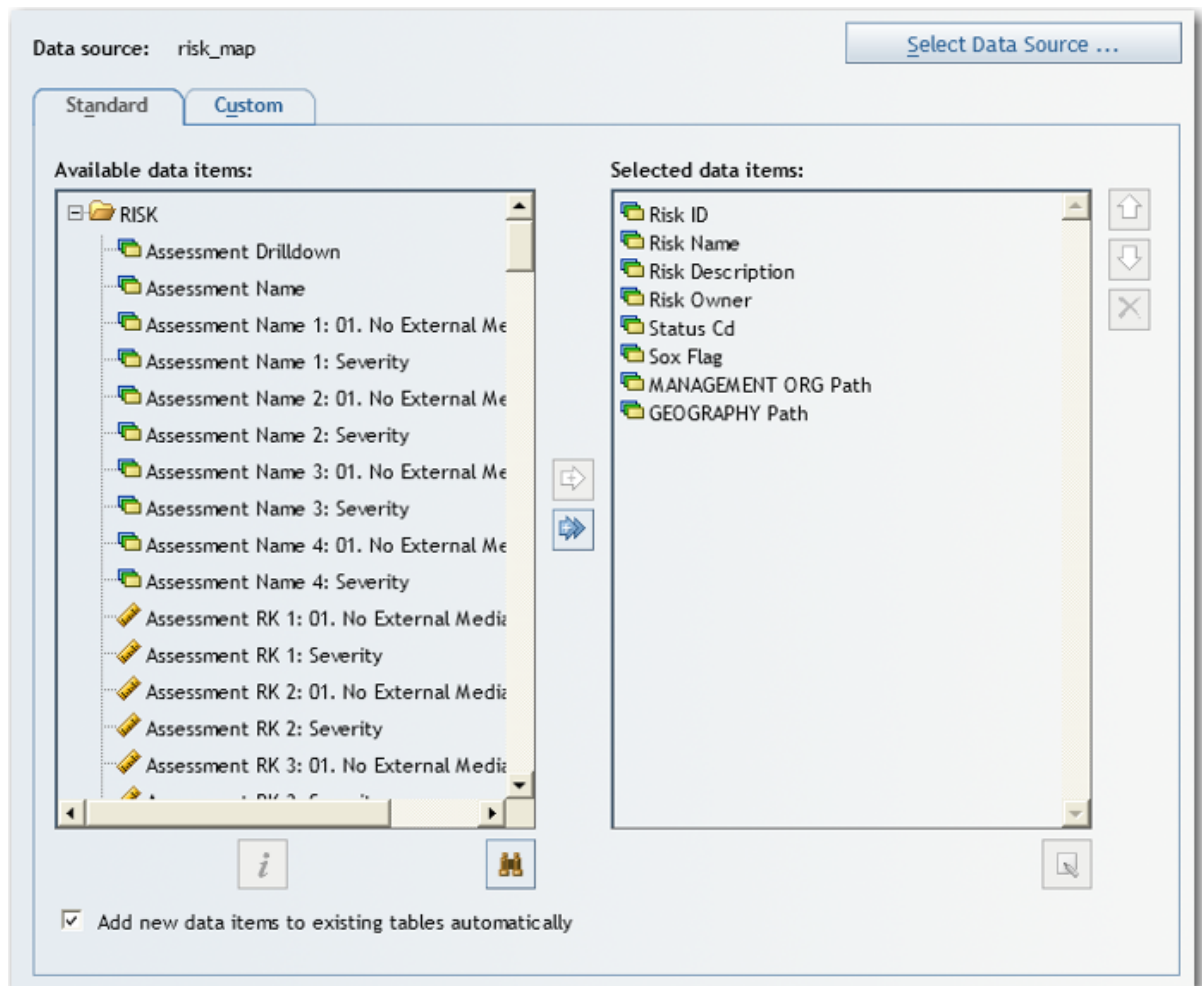
2. Click **New using Template**. The Template window appears.
3. On the Template window, click **Shared templates**. This tab contains the template that adds the operational location selector to the report.



4. Select the template that you want. In this example, select **EGRC risk_map**. The window that appears now has a stored process for displaying the operational location selector for the risk_map information map. It also has a table that shows where the map results will be displayed when data has been selected.



5. From the SAS Web Report Studio menu, select **Data > Select Data** to open data source for your report.
6. Click **Select Data Source**, and then navigate to the risk map: **SAS Folders > Products > SAS Enterprise GRC 6.1 > Reports > Risk Management > risk_map**. Click **OK** to select this information map.
7. In the Select Data window, expand **RISK** and move the data items that you want to display from **Available data items** to **Selected data items**.



In this example, we have selected **Risk ID, Risk Name, Risk Description, Risk Owner, Status Cd, Sox Flag, MANAGEMENT ORG Path, and GEOGRAPHY Path**. Click **OK**.

8. Click the **View** tab to view the results of the report that you are building.

Filter by Operational Area

Management Organization: (None Selected)
Geography: (None Selected)

Applied filters: None

Risk ID	Risk Name	Risk Description	Risk Owner	Status Cd	Sox Flag	MANAGEMENT ORG Path	GEOGRAPHY Path
CAN-3PARTY	Name of CAN-3PARTY	Description of CAN-3PARTY		Approved	Y	Superior Life > Canada	
CAN-ADQSKL	Name of CAN-ADQSKL	Description of CAN-ADQSKL		Approved	N	Superior Life > Canada	
CAN-CHANMAN	Name of CAN-CHANMAN	Description of CAN-CHANMAN		Approved	N	Superior Life > Canada	
CAN-DELFINREP	Name of CAN-DELFINREP	Description of CAN-DELFINREP		Approved	N	Superior Life > Canada	
CAN-FAILEXEC	Name of CAN-FAILEXEC	Description of CAN-FAILEXEC		Approved	N	Superior Life > Canada	
CAN-FAILSLA	Name of CAN-FAILSLA	Description of CAN-FAILSLA		Approved	N	Superior Life > Canada	
CAN-FLAWBUSP	Name of CAN-FLAWBUSP	Description of CAN-FLAWBUSP		Approved	N	Superior Life > Canada	
CAN-INADBCP	Name of CAN-INADBCP	Description of CAN-INADBCP		Approved	N	Superior Life > Canada	
CAN-INCLLAB	Name of CAN-INCLLAB	Description of CAN-INCLLAB		Approved	N	Superior Life > Canada	
CAN-INCTURN	Name of CAN-INCTURN	Description of CAN-INCTURN		Approved	N	Superior Life > Canada	
CAN-INSCAP	Name of CAN-INSCAP	Description of CAN-INSCAP		Approved	N	Superior Life > Canada	
CAN-INSUFAP	Name of CAN-INSUFAP	Description of CAN-INSUFAP		Approved	N	Superior Life > Canada	

Note that the view shows the operational location selector so that you can filter the report by operational location.

Note: In order for a user to see the operational location selector in SAS Web Report Studio, a user must be granted the local security permission **Log on as a Batch Job** by a system administrator on the server tier machine.

- On the operational location selector, click **Edit**. Select an operational location. For example, select **Management Organizations > Superior Life > Canada**. Click **OK**. The report then filters criteria by location.

Filter by Operational Area

Management Organization: Superior Life > Canada
Geography: (None Selected)

Applied filters: None

Risk ID	Risk Name	Risk Description	Risk Owner	Status Cd	Sox Flag	MANAGEMENT ORG F
CAN-3PARTY	Name of CAN-3PARTY	Description of CAN-3PARTY		Approved	Y	Superior Life > Canada
CAN-ADQSKL	Name of CAN-ADQSKL	Description of CAN-ADQSKL		Approved	N	Superior Life > Canada
CAN-CHANMAN	Name of CAN-CHANMAN	Description of CAN-CHANMAN		Approved	N	Superior Life > Canada
CAN-DELFINREP	Name of CAN-DELFINREP	Description of CAN-DELFINREP		Approved	N	Superior Life > Canada
CAN-FAILEXEC	Name of CAN-FAILEXEC	Description of CAN-FAILEXEC		Approved	N	Superior Life > Canada
CAN-FAILSLA	Name of CAN-FAILSLA	Description of CAN-FAILSLA		Approved	N	Superior Life > Canada
CAN-FLAWBUSP	Name of CAN-FLAWBUSP	Description of CAN-FLAWBUSP		Approved	N	Superior Life > Canada
CAN-INADBCP	Name of CAN-INADBCP	Description of CAN-INADBCP		Approved	N	Superior Life > Canada
CAN-INCLLAB	Name of CAN-INCLLAB	Description of CAN-INCLLAB		Approved	N	Superior Life > Canada
CAN-INCTURN	Name of CAN-INCTURN	Description of CAN-INCTURN		Approved	N	Superior Life > Canada
CAN-INSCAP	Name of CAN-INSCAP	Description of CAN-INSCAP		Approved	N	Superior Life > Canada
CAN-INSUFAP	Name of CAN-INSUFAP	Description of CAN-INSUFAP		Approved	N	Superior Life > Canada

- To save this report as a SAS Web Report Studio report, select **File > Save As**. Enter a **Name** for the report, navigate to the appropriate directory (for example, SAS

Folders > Products > SAS Enterprise GRC 6.1 > Reports > Risk Management) and click **Save**. You can then access and run the report from the SAS Enterprise GRC application.

Name: Risk Report for Canada x

Type: Data is automatically refreshed v

Location:

Risk Management Show description

Name	Author	Date	Keywords
cause_map		7/12/2013	
control_map		7/12/2013	
Risk Heat Map		7/12/2013	
risk_indicator_map		7/12/2013	
risk_map		7/12/2013	
test_wrs_report	admin	7/19/2013	

Description:

Keywords:

☐ Retain assigned group break values

☐ Automatically replace if file already exists ☐ Make read-only

Save **Cancel**

Example: Launching a SAS Business Intelligence Dashboard

This example demonstrates how to launch the `risk_indicator_dashboard`, which displays information about categorized risk indicators. By default, the risk indicator dashboard is commented out of the user interface. For more information about enabling the risk indicator dashboard, see “Modify the HomePage.xml Screen Definition to View the BI Dashboard in the User Interface” in the *SAS Enterprise GRC: Installation and Configuration Guide*.

To launch the `risk_indicator_dashboard` BI dashboard element:

1. Navigate to the **Risk Management** reports folder in SAS Enterprise GRC.
2. Click **risk_indicator_dashboard** to launch SAS BI Dashboard and view the dashboard element.

To manage a dashboard, click **Manage Dashboards** to launch the SAS BI Dashboard Designer.



For more information about using SAS Business Intelligence Dashboard, see the *SAS BI Dashboard: User's Guide*.

Appendix 1

Performing Other Administrative Tasks

Overview	195
Viewing Link Types	196
Managing Screen Definitions	196
Viewing Documentation on Components, Functions, Directives, and Properties	197
Flushing Caches	197
Viewing Configuration Details	197
Managing Locked Objects	198
Viewing Logon Activities	198
Loading, Unloading, and Exporting Data	199
Overview	199
Loading Data	199
Unloading Data	200
Exporting Data for Data Loading	201
Example: Data Loading Questions and Question Groups for a Questionnaire-Based Assessment	201

Overview

This chapter is intended to provide information to administrators on using the default user interface to perform the following administrative tasks in SAS Enterprise GRC:

- [Viewing Link Types](#)
- [Managing Screen Definitions](#)
- [Viewing Documentation on Components, Functions, Directives, and Properties](#)
- [Flushing Caches](#)
- [Viewing Configuration Details](#)
- [Managing Locked Objects](#)
- [Viewing Logon Activities](#)
- [Loading, Unloading, and Exporting Data](#)

For more information about the process of gathering organizational data, see [Chapter 3](#), “Gathering Governance, Risk, and Compliance Data,” on page 27.

This chapter uses the default environment for the example provided in [Chapter 3, “Gathering Governance, Risk, and Compliance Data,”](#) on page 27. The example environment is based on the sample data that is provided with the product. Your organization's tasks might vary depending on the level of customization. For more detailed information about administrative tasks such as product installation, customization, configuration, assigning roles and permissions to users, and data management, see the *SAS Enterprise GRC: Administration and Customization Guide*.

Viewing Link Types

Link types enable administrators to define which objects can be linked to each other. For example, KRIs can be linked to controls, and so on. To view link types that have been data loaded, select **Administration > Link Types** from the menu. This window is read-only. In order to create or delete link types from the system, you must use the LinkTypes data loader or unloader.

For more information about using the data loaders, see [“Loading, Unloading, and Exporting Data”](#) on page 199 or refer to the “Customizing SAS Enterprise GRC” chapter in the *SAS Enterprise GRC: Administration and Customization Guide*.

Managing Screen Definitions

Many windows in SAS Enterprise GRC can be customized using a screen definition file. This file is an xml file that contains programming statements that control how the application displays the window and how the user can interact with the window. For information about programming the screen definition file, see “Custom Page Builder” in the *SAS Enterprise GRC: Administration and Customization Guide*.

You must have the Load and Update Screen Definitions for Custom Page Builder global capabilities to view the Screen Definitions window.

An attribute of the screen definition file is the screen definition type. You can have multiple screen definitions that all have the same screen definition type. However, only one screen definition can be active at a time for any given screen definition type. You should always have an active screen definition for each screen definition type. If you do not have an active screen definition for a screen definition type, then the corresponding window cannot be displayed in the application.

To view information about screen definition types, select **Administration > Screens > Screen Definition Types** from the menu.

It is strongly recommended that you do not edit the sample screen definition files. If you want to create your own file, it is recommended that you copy the sample file to a different name and apply a different ui-definition ID as defined in the XML file. You can then use the copy as a template for your new screen definition file.

To upload a screen definition file:

1. Select **Administration > Screens > Screen Definitions** from the menu. Click **Upload Definition** to upload a definition. The Upload Screen Definition File window appears.
2. Click **Browse** to select a screen definition file from your local file system.
3. Click **Upload**.

Viewing Documentation on Components, Functions, Directives, and Properties

Administrators can view information about components, functions, directives, and properties from the **Administration > Screens** submenu. This information can be used when customizing SAS Enterprise GRC.

To view component documentation, select **Administration > Screens > Component Documentation** from the menu.

To view function documentation, select **Administration > Screens > Function Documentation** from the menu.

To view directive documentation, select **Administration > Screens > Directive Documentation** from the menu.

To view the properties that exist in the SAS Enterprise GRC system and their values, select **Administration > Screens > Properties Documentation** from the menu.

Flushing Caches

The Flush Caches window can be used to flush caches. This action clears all the cached data that is associated with the user's server-side session. This enables an administrator to make customizations or configuration changes without requiring a restart of the Web application server.

You must have the Super-User global capability to view the Flush Caches window.

To flush caches:

1. Select **Administration > Site Maintenance > Flush Caches** from the menu. The Flush Caches window appears.
2. Click **Flush Caches** to flush all caches.

Viewing Configuration Details

The Configuration Details window shows the configuration options that have been explicitly set in configdata.properties.

You must have the Super-User global capability to view the Configuration Details window.

To view configuration details:

1. Select **Administration > Site Maintenance > Configuration Details** from the menu. The Configuration Details window appears.
2. View the configuration details. To view details about the configuration of dimensions, click **dimensionality.xml**.

Modifying configuration details must be performed outside of the user interface. For more information, see the *SAS Enterprise GRC: Administration and Customization Guide*.

Managing Locked Objects

The Locked Objects window enables you to unlock data objects. This feature is useful if users are sharing objects. For example, if a user leaves the office for a week with an object open for editing, then no other user can use that object until the user returns and finishes editing the object. This window can be used to unlock the object without having to wait for a user to return.

Note: When you unlock an object while a user is currently editing the object, any changes the user has made to that object will not be saved and the object will not advance in the workflow.

You must have the Super-User global capability to view the Locked Objects window.

Suppose that Jacques is editing an issue. This issue is locked and cannot be edited by anyone else. An administrator can unlock the issue using the following steps:

1. Log in as an administrator. Select **Administration > Site Maintenance > Locked Objects** from the menu. The Locked Objects window appears.

Display A1.1 Example of a Locked Object

Filter by Operational Area Edit Clear Favorites▼						
Management Organization: (None Selected)						

Locked Objects Unlock Selected						
	Current User	Object ID	Object Last Modified	Name or Title ▲	Current User Last Logged On	Object Last Locked
1	rdt0020 - Central Risk Management	10761	April 25, 2014 11:51:03 AM EDT	bw test	April 25, 2014 11:50:53 AM EDT	April 25, 2014 11:51:05 AM EDT

Rows 1 to 1 of 1

2. Select the object type, in this case **Issue**, in the **Object Type** field, and then click **Go**.
3. Check the issue that you want to unlock and click **Unlock Selected**. Click **OK** to unlock the object.

To view the object, click an attribute of that object in the table. The object opens in the corresponding window.

Viewing Logon Activities

Every time a user logs on to the Web application, a record is kept. This record contains the user ID and the datetime value. To access logon information, select **Administration > Site Maintenance > Logon Activity** from the menu.

Loading, Unloading, and Exporting Data

Overview

Administrators can load (create), unload (delete), and export data in SAS Enterprise GRC data through the user interface.

Data loaders are used to load and unload data. To access the data loader, select **Administration > Data > Load** from the menu. To access the data unloader, select **Administration > Data > Unload** from the menu.

SAS Enterprise GRC data loaders load most of the information that is required by the system and all of the information that is created by the system. By using these data loaders, you can load a large amount of data without tedious and repetitive manual entry. The versatility of data loading in bulk also enables you to localize column headings, load several files that are related using a single spreadsheet, and easily load data from different branches of an organizational tree. This is done through the Load window. There is also an option to load data via the command prompt. For more information about loading data via command prompt, see the *SAS Enterprise GRC: Administration and Customization Guide*.

Some caveats apply to data loading. For policies, test definitions, and tests that are loaded into the system via data loaders, these loaded objects do not appear in the task list of an assigned user until the object is viewed through the user interface. Viewing the object then initiates the workflow and results in a task list item for the applicable party. For example, a test that has been “accepted” by a tester via a data loader does not appear in the task list of the tester (the workflow does not “start”) until the test has been accessed from the Tests window. Testing in this case applies both to audit management and control testing.

You can also export data for data loading. Exporting data essentially copies the data into an Excel file that can be used for data loading.

Loading Data

To load data from a spreadsheet into SAS Enterprise GRC:

1. Select **Administration > Data > Load** from the menu. The Load window appears.
2. (Optional) Click **View Available Loaders**. A list of the available data loaders is displayed. Click on a specific data loader to view the columns that can be loaded or to download a sample spreadsheet. The locale-independent sample spreadsheets contain the column identifiers. The locale-specific sample spreadsheets contain local column names.

You can use the sample spreadsheets to create and build the set of data that you want to load into the system.

For more descriptive information about data loaders, see the *SAS Enterprise GRC: Administration and Customization Guide*.

3. Click **Browse** to select an Excel Workbook from your local file system.
4. Select one of the following data-loading options:

- Select **Test Mode** in order to process a workbook but not save any of its data to the database. This selection enables you to check a workbook for errors without performing an actual upload.
 - Select **Reject entire workbook on error** in order to process a workbook only until an error occurs. If an error occurs, no data is saved to the database.
 - Select **Reject worksheet on error** in order to process a workbook but reject any spreadsheets in which an error occurs.
 - Select **Process all valid records** in order to process a workbook and save all of its data. Any records with errors are skipped and not loaded. A results file is created which contains a separate sheet for all erroneous records in the workbook that failed during the data load, so that you can correct and upload them again.
5. Select whether you want to enable alert notifications for the objects you load. In order for this option to be enabled, alert notifications must be specified in the Configuration Manager (which is the default setting). Some loaded data can trigger alert notifications, such as e-mail messages, to applicable parties within a specified object. When loading a large number of objects, this can result in performance issues.
 6. Select whether you want to validate operational locations for items you are loading. In order for this option to be enabled, location validation must be specified in the Configuration Manager (by default, this is set to **No**). This option checks to see if any dimensions you are loading into the system are not allowed for a particular business object, or if any required dimensions were not specified in workbook entries. For example, if Management Organization and Geography are the only valid dimensions for a particular business object, adding a business object that includes the Business Line dimension will fail. Likewise, trying to add a business object with a required dimension like Management Organization will fail if the management organization is not specified in the workbook entry.
 7. Click **Upload**.

Note: Data loader names are case-sensitive. Therefore, the name of the Excel worksheet within the Excel workbook must match the loader name exactly.

Unloading Data

When you unload data in SAS Enterprise GRC, you are deleting individual records from SAS Enterprise GRC. In this case, deleting data means that these records are no longer visible through the user interface; however the system still maintains a full audit trail. The format for unloading data is the same as that for loading data.

To unload data from SAS Enterprise GRC:

1. Select **Administration > Data > Unload** from the menu. The Unload window appears.
2. (Optional) Click **View Available Unloaders**. A list of the available data unloaders is displayed. Click on a data unloader to view the columns that can be unloaded or to download a sample spreadsheet. The locale-independent sample spreadsheets contain the column identifiers. The locale-specific sample spreadsheets contain local column names.

For more descriptive information about data unloaders, see the *SAS Enterprise GRC: Administration and Customization Guide*.


3. Click **Browse** to select an Excel Workbook from your local file system.

4. Select one of the following data-unloading options:
 - Select **Test Mode** in order to process a workbook but not deactivate any of its data in the database. This selection enables you to check a workbook for errors without performing an actual deactivation.
 - Select **Reject entire workbook on error** in order to process a workbook only until an error occurs.
 - Select **Reject worksheet on error** in order to process a workbook but reject any spreadsheets in which an error occurs.
 - Select **Process all valid records** in order to process a workbook and deactivate all of its data. Any records with errors are skipped and not unloaded.
5. Click **Unload**.

Note: Data unloader names are case-sensitive. Therefore, the name of the Excel worksheet within the Excel workbook must match the unloader name exactly.

Exporting Data for Data Loading

To export data from SAS Enterprise GRC into a spreadsheet that you can use to load or unload data, do the following:

1. Select an applicable window that contains exportable business objects. For example, if you want to export assessment data, select **Risk Management > Assessments** from the menu. The Assessments window appears.
2. Click the down arrow () next to **Menu**, and select **Export for Dataload**.
3. Select options for exporting the data:
 - Select **Export dimension details** if you want to include dimensional details included in the output file.
 - Select **Export displayed columns only** if you want to only include columns that appear by default in the user interface.
4. Click **OK** to begin exporting and downloading the file.

Note: This process could take some time depending on the amount of data being exported.

Example: Data Loading Questions and Question Groups for a Questionnaire-Based Assessment

In this example, Orion Star is using the data loader to load questions and a question group for a questionnaire-based assessment that asks about control effectiveness. The following table shows the information that must be loaded for the question group. Leave all other fields blank.

Question Group Column Name	Column Value
businessObjectLocalization.nameTxt	<i>Internal Fraud Exposure Group</i>

Question Group Column Name	Column Value
businessObjectLocalization.descTxt	<i>This question group is designed to ask questions about internal securities fraud exposures.</i>
assessmentQuestionGroup.assessmentGroupId	Fraud-001
assessmentQuestionGroup.sourceSystemCd	MON
assessmentQuestionGroup.activeFlg	true

The following table shows the information that must be loaded for the two questions in the question group. Column values should be entered per row.

Question Column Name	Column Value
assessmentQuestionGroup.sourceSystemCd	MON MON
assessmentQuestionGroup.assessmentGroupId	<i>Fraud-001</i> <i>Fraud-001</i>
assessmentQuestion.assessmentQuestionId	<i>IF-Q1</i> <i>IF-Q2</i>
assessmentQuestion.sourceSystemCd	MON MON
assessmentQuestion.displayStyle	NUM NUM
businessObjectLocalization.nameTxt	<i>Provide your assessment of average loss.</i> <i>Provide your assessment of risk of loss.</i>
businessObjectLocalization.descTxt	<i>What is the estimated average loss from this type of fraud event?</i> <i>How high is the risk of direct financial loss from this type of fraud event?</i>
questionGroupMapping.orderNo	2 1
responseScale.responseScaleId	EFF EFF
responseScale.sourceSystemCd	MON MON

To load questions and question groups into the system, do the following as Administrator:

1. Select **Administration > Data > Load** from the menu.
2. Click **View Available Loaders**. A dialog box with a list of the available data loaders is displayed. Click the **AssessmentQuestionGroups** loader and select **locale-independent** to download the sample spreadsheet. Click **OK**.
3. Click the **AssessmentQuestions** loader and select **locale-independent** to download the sample spreadsheet. Click **OK**. Close the Available Loaders dialog box to return to the Load window.
4. Open each spreadsheet, enter row data using the sample information from the preceding tables, and then save the spreadsheets.
5. On the Load window, click **Browse** and select the assessment question groups spreadsheet that you saved. Select **Reject entire workbook on error** in order to process a workbook only until an error occurs. Click **Upload**. If an error occurs, no data is saved to the database.
6. Repeat the preceding step for the assessment questions spreadsheet.
7. To ensure you have properly added the items in question, select **Risk Management > Libraries** from the menu and click the **Questions** and **Question Groups** links on the left pane, respectively. The items that you have created should appear in these library tables.

Glossary

action plan

an outline of a strategy for resolving an issue. For example, an action plan could be created to update a building's security system in order to address an issue with after-hours equipment theft.

activity status

the condition of a dimensional element or data object being active, inactive, or staged. In some cases, the activity status is determined by an active period that is bounded by a beginning date and an ending date.

allocation

a portion of the net financial impact of an incident that is attributed on the accounting books to a particular operational risk location. The net financial impact of an incident can be allocated to multiple operational risk locations across an organization.

assessable

See assessment item.

assessable type

a particular type of risk, cause, or control for which an assessment is conducted. For example, a bank vault is a type of control intended to secure valuables.

assessment item

the specific risk, cause, control, or potential impact that is being assessed. In the case of a bank vault control, the item to be assessed could be the bank vault at a specific bank.

assessment template

a tool that is used to create several assessments that have some data objects in common, such as assessors and pre-populated risks. The data objects in common are part of the planning and scoping stages of the assessment.

assessor

a user who provides responses to a questionnaire.

audit

the formal examination and evaluation of an organization's controls to ensure organizational compliance.

audit mission

a record that captures all of the details associated with the execution of an individual audit.

bucket

a continuous range of severity values.

cause

a primary factor that leads to an operational failure or loss event, and in turn to losses.

cause weight

a percentage that indicates the contribution of a cause relative to all of the causes for an incident.

control certification

an evaluation of a control for a control-testing measure during a specific time period.

control certification period

the span of time for which a control is certified.

control instance

a combination of a control type and the operational risk point to which it applies.

control profile

a list of controls for a given operational area. The controls can be entered directly or as part of an assessment.

control testing measure

a process used to evaluate an attribute of a control.

control testing responses

a list of possible values for a control testing measure.

data loader

the component that loads data files for manipulation in the user interface.

data unloader

the component that deactivates data files in the user interface.

dimensional element

a classification in a dimensional hierarchy.

dimensional hierarchy

a taxonomy for a specific category of items, arranged by parent-child relationships, in the organizational, operational, or risk management practices of an institution.

effect amount

a record of individual amounts associated with a financial effect.

financial effect

a loss, gain, or near-miss. A financial effect can contain multiple effect amounts.

governance

the setting and imposing of effective, ethical, and measurable processes, rules, regulations, and guidelines to ensure proper management of an organization

incident

an object used to record an event and to account for things associated with the event such as financial effects, nonfinancial effects, recoveries, allocations, causes, and failed controls.

inherited mapping

a mapping that applies to a dimensional element because it is defined higher up in the dimensional hierarchy, rather than because it is defined exactly at the element.

investigator

a user who is responsible for researching and entering the details of an event.

issue

a statement of an item that needs attention.

issue threshold

a predetermined cut-off value that can be used on the Incident Management tab. When the threshold is breached, an issue is created automatically.

Key Risk Indicator

a variable that is used as an early warning signal of an operational risk exposure. A KRI might affect the level of operational risk exposure. It is used in estimating the likelihood and severity of the exposure. Short form: KRI.

KRI

See Key Risk Indicator.

KRI definition

a template for creating key risk indicators.

KRI observation

the value of a key risk indicator during a specified reporting period.

KRI request

a short survey that is sent to the owner of a key risk indicator for the purpose of collecting one observation for that indicator.

level

an element of a dimension hierarchy. Levels describe the dimension from the highest (most summarized) level to the lowest (most detailed) level. For example, possible levels for a Geography dimension are Country, Region, State or Province, and City.

management validation

the validation by local managers that confirms the occurrence and details of a loss, a recovery, or an event.

measure

a risk metric in an organization. Examples of measures include VaRs in simulations, gammas in sensitivities, and PLs in scenarios.

navigation tree

a visual representation of a dimensional hierarchy.

nonfinancial effect

an effect (such as enhanced corporate reputation) of an operational risk that is not directly recorded on an organization's financial statement.

notify list

the set of users who will be automatically contacted when the assessment or scenario questionnaires are distributed.

operational risk area

a set of operational risk points that is defined either by directly specifying the set of points individually or by specifying a set of dimensional elements, possibly including more than one element from a single dimension. In the latter case, the area consists of every point that can be constructed from all possible combinations of the specified elements.

operational risk point

a single point in the multidimensional space of an organization that consists of a set of dimensional elements that are taken from distinct dimensions. An operational risk point cannot refer to two elements in the same dimension, but it might implicitly include all the descendents of an element.

originator

a user who submits a data object for validation.

period

the unit of time for which an assessment or scenario is conducted.

policy

a formal statement of guidelines. Organizations define policies to ensure compliance with laws and regulations, reduce risk, and align actions and decisions with organizational values and objectives.

potential impact

the amount exposed to a particular risk that is associated with a specific operational location.

question group

a set of related questions about an assessment item.

questionnaire

a specific set of question groups that is intended to be completed by assessors who have specific positions within an organization.

questionnaire template

a general set of question groups from which a questionnaire can be created.

recovery

an accounting object that reduces the impact of a financial effect. A recovery can be either a direct recovery or an insurance recovery.

recovery amount

a record of individual amounts associated with a recovery.

relative weight

a number indicating the relative contribution of an assessment question to the total score calculated for an assessment question group. Also, the relative contribution of assessment scores collected for a type of item (such as control) to a combined score computed for another type of item (such as risk).

risk instance

the combination of an event risk category and the operational risk point to which it is relevant.

risk profile

the set of measure scores that is associated with a specific risk instance. These scores can be calculated as a result of an assessment, or they can be entered directly.

risk validation

the validation by central risk managers that confirms that a record indicates a risk within the organization.

role

See user role.

source system

the type of database from which operational loss data originates or to which it is being exported.

staged

a condition indicating that a data object is not currently active but is scheduled to become active on a future date.

test definition

a template used to create tests.

test definition group

a group that contains several test definitions. All test definitions within a given group must have the same control testing measure.

test period

span of time for which a control is tested.

user role

a set of permissions that define which actions a user, or a group of users, can take in an application.

validation stage

a step in a validation workflow that is mapped to an operational risk location and its associated positions. At a validation stage, a data entry or questionnaire response can be validated and sent to the next stage or returned to assessors for re-entry of responses.

validation workflow

the series of steps through which a data entry or questionnaire response is approved.

validator

a user who verifies the validity of a data entry or a questionnaire response.

Index

A

- access [5](#)
- activity status [23](#)
- administrative tasks
 - exporting data [201](#)
 - loading data [199](#)
 - managing locked objects [198](#)
 - managing screen definitions [196](#)
 - overview [195](#)
 - performing site maintenance [197](#)
 - unloading data [200](#)
 - viewing configuration details [197](#)
 - viewing link types [196](#)
 - viewing logon activities [198](#)
- assessment example [156](#)
 - approving form-based assessment completion [160](#)
 - approving form-based assessment plan [159, 166](#)
 - assessing risk [159, 166](#)
 - creating new form-based assessment [157](#)
 - creating questionnaire-based assessment [165](#)
 - form-based assessment process [157, 162](#)
 - form-based assessment workflow [156](#)
 - questionnaire-based assessment workflow [161](#)
 - responding to risk results [160, 167](#)
- assessment workflows
 - overview [145](#)
- assessments [144](#)
 - defining data objects [151](#)
 - direct-edit process [151](#)
 - form-based assessment process [148](#)
 - form-based assessment roles [146](#)
 - other assessment-related roles [147](#)
 - overview [145](#)
 - questionnaire-based assessment process [150](#)

- questionnaire-based assessment roles [147](#)

- questionnaire-based implementation [152](#)

- audit management [123](#)

- lifecycle [125](#)
- overview [124](#)
- roles [125](#)

- audit management example [127](#)

- approving audit mission [129, 130](#)
- approving audit test results [131](#)
- approving completed audit mission [131](#)
- creating audit mission [128](#)
- performing audit [131](#)
- publishing audit tests [130](#)
- workflow [127](#)

- availability [5](#)

B

- business model [4](#)

C

- cause [145](#)
- cause type [145](#)
- compliance [5](#)
- confidentiality [5, 25](#)
- control [145](#)
- control testing [111](#)
 - controls and control testing workflows [112](#)
 - definitions [112](#)
 - process [114](#)
 - roles [113](#)
- control testing example [115](#)
 - accepting and completing test [120](#)
 - approving a control [121](#)
 - approving a test definition [119](#)
 - approving test results [120](#)
 - approving the control [118](#)

- certifying a control [121](#)
- creating a control [117](#)
- creating a test [119](#)
- creating a test definition [118](#)
- defining data objects [117](#)
- workflow [115](#)
- control type [145](#)
- currencies [70](#)
- currency conversion, automatic [26](#)

D

- data objects
 - activity of [24](#)
 - lock [24](#)
- data objects, frozen [24](#)
- data quality [4](#)
- dimension browser [50](#)
 - overview [50](#)
- dimensions
 - activity of [23](#)

E

- example
 - locked objects [25](#)
- example entity [28](#)
 - architecture [28](#)
 - business line chart [31](#)
 - business structure [30](#)
 - defining KRIs [42](#)
 - defining policies [36](#)
 - defining scenarios [39](#)
 - defining users, roles, and responsibilities [32](#)
 - developing assessments and assessment templates [38](#)
 - developing audits [45](#)
 - developing controls [43](#)
 - dimensionality [28](#)
 - geography chart [31](#)
 - issues and action plans [41](#)
 - management organization chart [30](#)
 - managing incidents [45](#)
 - mapping processes and workflows [35](#)
- exchange rates [71](#)
 - example calculation [71](#)

F

- financial data [70](#)

G

- gathering GRC data
 - overview [27](#)

- general features [14](#)
- GRC
 - Overview [27](#)

H

- help and more information [12](#)
 - About SAS Enterprise GRC window [13](#)
 - Help Menu [12](#)
- Home page [9](#)

I

- incident management [169](#)
 - classification [174](#)
 - definitions [171](#)
 - incident approval [178](#)
 - issue threshold example [177](#)
 - issue thresholds [176](#)
 - monetary breakdown [174](#)
 - overview [170](#)
 - roles [172](#)
 - workflow [173](#)
- incident management example [179](#)
 - approving event [183](#)
 - approving incident data [183](#)
 - business process [179](#)
 - completing an investigation [182](#)
 - creating a validation workflow [180](#)
 - creating an incident [181](#)
- insurance policies
 - example policy [73](#)
 - implementing [72](#)
- integrity [4](#)
- issues and action plans [87](#)
 - lifecycle [89](#)
 - overview [88](#)
 - roles [88](#)
- issues and action plans example [91](#)
 - accepting an issue [94](#)
 - approving action plan closure [96](#)
 - approving action plan completion [95](#)
 - approving an action plan [95](#)
 - approving an issue [94](#)
 - approving issue closure [96](#)
 - closing an issue [96](#)
 - completing an action plan [95](#)
 - creating an issue [93](#)
 - developing an action plan [94](#)
 - workflow [91](#)

K

- key features [2](#)
- Key Risk Indicators [97](#)
- KRI [97](#)

- Overview 98
- roles 99
- scoring 106
- workflow 100
- KRI example 100
 - creating a KRI 104
 - creating a KRI definition 102, 103
 - creating a KRI observation request 105
 - creating a validation workflow 102
 - providing a KRI score 105
 - reviewing a KRI score 105
 - submitting a KRI score 106
 - workflow 100

L

- logging off 8
- logging on 8

M

- mappings 59
 - adding item process mapping 60

N

- nodes
 - creating a merge file 57
 - creating a node 52
 - creating a split file 55
 - merging 56
 - moving a node 53
 - splitting nodes 54

O

- objectives 62
 - creating an objective instance 62
- objects
 - searching 13
- obligations 63
 - creating an obligation instance 63
- OL chooser
 - filtering 19
 - modes 17
 - using 16
- operational location 16
 - overview 16
- overview
 - SAS Enterprise GRC 1

P

- policy management 77
 - lifecycle 80
 - overview 78

- roles 79
- policy management example 81
 - approving a policy 84
 - approving policy expiration 85
 - communicating policy 85
 - creating a policy 83
 - expiring policy 85
 - providing a policy response 85
 - requesting responses 84
 - reviewing responses 85
 - workflow 81
- preferences
 - changing 11
- processes 61
 - creating a process instance 62

R

- reference numbers 23
- reporting 185
 - financial effects matrix report 188
 - information map 189
- risk 145
- risk assessment
 - creating questionnaire template 164
- risk event type 145
- risk example
 - approving new risk 155
 - business process 153
 - creating new risk 154
 - fully approving new risk 155
 - steps 154
- risk management challenges 4
- roles
 - assigning users 67
 - audit management 125
 - control testing 113
 - form-based assessments 146
 - incident management 172
 - issues and action plans 88
 - KRI 99
 - policy management 79
 - scenarios 134

S

- SAS Enterprise GRC
 - using 7
- scenario example 136
 - approving scenario responses 142
 - closing a scenario 142
 - completing a scenario questionnaire 141
 - creating a scenario 140
 - creating a scenario template 139
 - creating a scenario workflow 138, 163

- workflow 136
- scenarios 133
 - overview 134
 - roles 134
 - workflow 135
- search 13
- security 5
- settings
 - changing 11
- split file
 - creating a split file 55
- supported data sources 4
- supported data types 3

U

- user interface
 - icons 15

- linked objects graph 20
- navigating 14
- OL chooser 16
- OL chooser modes 17
- operational location 16
- structure of 14
- table functions 15
- view bar 20
- users and roles
 - assigning role and scope 67
 - implementing roles 66
 - implementing users 66
 - overview 65

V

- views
 - configuring 20