

Oracle® Internal Controls Manager

Implementation Guide

Release 11*i*

Part No. B12267-04

June 2005

Primary Author: Jacob John

Contributing Author: Nigel King, Bastin Gerald, Suraj Dyre, Sayekumar Arumugam, Mumu Pande, Qingdi Liu, Amit Bedajna, Tsun-Tsun Ho, Gaurav Kumar, Nilesch Panandikar, Krishnan Nair, Anisha Malhotra

The Programs (which include both the software and documentation) contain proprietary information; they are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright, patent, and other intellectual and industrial property laws. Reverse engineering, disassembly, or decompilation of the Programs, except to the extent required to obtain interoperability with other independently created software or as specified by law, is prohibited.

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. This document is not warranted to be error-free. Except as may be expressly permitted in your license agreement for these Programs, no part of these Programs may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose.

If the Programs are delivered to the United States Government or anyone licensing or using the Programs on behalf of the United States Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS

Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the Programs, including documentation and technical data, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement, and, to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software–Restricted Rights (June 1987). Oracle Corporation, 500 Oracle Parkway, Redwood City, CA 94065.

The Programs are not intended for use in any nuclear, aviation, mass transit, medical, or other inherently dangerous applications. It shall be the licensee's responsibility to take all appropriate fail-safe, backup, redundancy and other measures to ensure the safe use of such applications if the Programs are used for such purposes, and we disclaim liability for any damages caused by such use of the Programs.

The Programs may provide links to Web sites and access to content, products, and services from third parties. Oracle is not responsible for the availability of, or any content provided on, third-party Web sites. You bear all risks associated with the use of such content. If you choose to purchase any products or services from a third party, the relationship is directly between you and the third party. Oracle is not responsible for: (a) the quality of third-party products or services; or (b) fulfilling any of the terms of the agreement with the third party, including delivery of products or services and warranty obligations related to purchased products or services. Oracle is not responsible for any loss or damage of any sort that you may incur from dealing with any third party.

Oracle, JD Edwards, PeopleSoft, and Retek are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Contents

Send Us Your Comments

Preface

1 Introduction to Oracle Internal Controls Manager

| | |
|--|------|
| Introduction | 1-1 |
| Corporate Governance | 1-1 |
| Overview of Oracle Internal Controls Manager | 1-4 |
| Setup of Oracle Internal Controls Manager. | 1-5 |
| Application Controls Monitoring | 1-8 |
| Integration with E-Business Suite Applications. | 1-9 |
| Responsibilities in Oracle Internal Controls Manager | 1-11 |

2 Processes and Organizations in Oracle Internal Controls Manager

| | |
|---|------|
| Introduction | 2-1 |
| Overview of Process Setups in Oracle Internal Controls Manager. | 2-1 |
| Creating Processes directly within Oracle Internal Controls Manager | 2-4 |
| Importing Process Documents using Oracle Tutor. | 2-5 |
| To Import Process Documents using Tutor. | 2-5 |
| To Import Process Flow Diagrams using Tutor | 2-9 |
| Importing Processes using Oracle Workflow | 2-9 |
| To import processes using Oracle Workflow | 2-10 |
| Importing Processes using Web ADI. | 2-12 |
| To Import Processes using Web ADI | 2-13 |
| Process Objectives. | 2-17 |
| Setting up Process Objectives | 2-17 |
| Process Attributes | 2-19 |
| Associating Documents with Processes | 2-22 |
| Tutor Attachments | 2-22 |
| Other Attachments | 2-23 |
| Linking Key Accounts with Processes | 2-25 |
| Pre-Requisites to linking Accounts and Processes. | 2-25 |
| Manually link Significant Accounts with Processes | 2-28 |
| Import the process and key account associations | 2-28 |
| Organizations in Oracle Internal Controls Manager | 2-29 |

| | |
|--|------|
| To Setup Organizations in Oracle Internal Controls Manager | 2-29 |
| Linking Processes with Organizations. | 2-31 |
| Linking Risks and Controls with Organizations | 2-34 |
| Viewing Organizations | 2-34 |

3 Process Approvals & Change Management

| | |
|--|-------------|
| Process Approvals in Oracle Internal Controls Manager | 3-1 |
| Process Verification. | 3-1 |
| Process Approval Setup - Process Parameters | 3-2 |
| Process Hierarchies. | 3-4 |
| Process Hierarchy Views | 3-7 |
| Process Approval Examples | 3-9 |
| Process Rejection | 3-11 |
| Process Revisions in Oracle Internal Controls Manager | 3-11 |
| Revising Processes in the Risk Library - Part 1 | 3-11 |
| Revising Processes in the Risk Library - Part 2 (Process Variation Management) | 3-12 |
| Revising Processes in Organizations | 3-16 |
| Process Revision Examples | 3-19 |
| Process Deletions (Removals and Disassociations) | 3-20 |
| Process Deletion Examples | 3-22 |
| Submitting Processes and Process Revisions for Approval | 3-23 |
| Setup for Process Approval | 3-24 |
| Enable Business Event Processing | 3-28 |
| Submit the Process for Approval | 3-28 |
| Process History | 3-29 |

4 Risks and Controls in Oracle Internal Controls Manager

| | |
|---|-------------|
| Overview of the Risk Library | 4-1 |
| Risks. | 4-2 |
| Setting up Risks in Oracle Internal Controls Manager | 4-2 |
| Risk Attributes. | 4-4 |
| Risks, Risk Types and Regulations | 4-5 |
| Risks and Risk Type | 4-5 |
| Risk Types and Regulations | 4-8 |
| Risks Search | 4-9 |
| Risk Views | 4-10 |
| Controls | 4-10 |
| Setting up Controls in Oracle Internal Controls Manager | 4-10 |
| Control Attributes | 4-11 |
| Controls Search | 4-17 |
| Importing Risks and Controls into Oracle Internal Controls Manager | 4-17 |
| Import Risks and Controls (into the Risk Library). | 4-19 |
| Import Risks and Controls in Organizations | 4-23 |
| Import Controls | 4-25 |
| Export Risk and Control Objects | 4-28 |

| | | |
|-----------|---|------|
| 5 | Audit Procedures in Internal Controls Manager | |
| | Introduction | 5-1 |
| | Setting up Audit Procedures in Oracle Internal Controls Manager | 5-2 |
| | Importing Audit Procedures into Oracle Internal Controls Manager | 5-5 |
| | Creating Audit Procedures within an Audit Engagement | 5-6 |
| 6 | Risk Library Change Control | |
| | Introduction | 6-1 |
| | Manage the Risk Library | 6-1 |
| | Certifying New Objects in the Risk Library | 6-2 |
| | Revising Objects in the Risk Library | 6-3 |
| | Approval and Revision Status Values | 6-4 |
| | Deletion of Approved Objects | 6-5 |
| 7 | Assessments in Oracle Internal Controls Manager | |
| | Introduction | 7-1 |
| | Integration with Oracle Scripting | 7-2 |
| | Creating an Assessment in Oracle Internal Controls Manager | 7-4 |
| | To Create an Assessment | 7-4 |
| 8 | Audit Engagements | |
| | Introduction | 8-1 |
| | Setup the Audit Engagement within Oracle Internal Controls Manager | 8-2 |
| | Setup the Audit Engagement through Integration with Oracle Projects | 8-10 |
| | Scoping the Audit Engagement | 8-13 |
| | Scoping with Companies, LOB's, Organizations, and Processes | 8-14 |
| | Scoping with Organizations and Processes only | 8-15 |
| | Notes on Scoping. | 8-17 |
| | Executing the Audit Engagement | 8-19 |
| | Notes on Engagement Execution | 8-28 |
| | Opinions Framework in Oracle Internal Controls Manager | 8-29 |
| 9 | Segregation of Duty Constraints | |
| | Introduction | 9-1 |
| | Responsibilities and Functions in Oracle Applications | 9-2 |
| | Implementing Segregation of Duties Constraints | 9-5 |
| | 1. Define Segregation of Duty Constraints | 9-6 |
| | 2. Check for Segregation of Duties Constraint Violations | 9-11 |
| | 3. Initiate Correction Requests (and Subsequently Modify User Duties) | 9-13 |
| 10 | Process and Organization Certification | |
| | Introduction | 10-1 |
| | Overview of Process / Organization Certification | 10-1 |

| | |
|--|-------|
| Corporate Processes vs. Organization (Local) Processes | 10-3 |
| Implementing Process / Org Certification in Oracle Internal Controls Manager. | 10-4 |
| Process / Org Certification: Global Operations Controller | 10-5 |
| 1. Review Certifications and their Current Evaluations | 10-5 |
| 2. Create a Certification and Set its Scope | 10-13 |
| 3. Send Notifications to Business Process Owners. | 10-16 |
| 4. Update Certification Status | 10-16 |
| Process / Org Certification: Business Process Owner. | 10-16 |
| Review Process and Org Certifications and Evaluations | 10-17 |
| Notify Sub-Process Owners | 10-17 |
| Link Assessments with Processes (Optional) | 10-17 |
| Evaluate Processes and Orgs. | 10-18 |
| Certify Processes and Orgs | 10-18 |
| Certification Notes. | 10-19 |
| Creating and Resolving Issues in Certification | 10-20 |

11 Financial Statement Certification

| | |
|--|-------|
| Introduction | 11-1 |
| Overview. | 11-1 |
| Setup of Financial Certifications in Internal Controls Manager | 11-3 |
| Certifying Financial Statements using Internal Controls Manager | 11-4 |
| 1. Create / Review Financial Certifications in the Enterprise | 11-5 |
| 2. Evaluate Financial Items | 11-9 |
| 3. Certify the Financial Statement. | 11-18 |

12 Findings in Oracle Internal Controls Manager

| | |
|--|-------|
| Introduction | 12-1 |
| Findings in Oracle Internal Controls Manager | 12-1 |
| Findings Types. | 12-2 |
| Setup of Findings | 12-3 |
| Recording Findings in Oracle Internal Controls Manager | 12-9 |
| Working with Findings in Oracle Internal Controls Manager | 12-11 |
| Using Remediations in closing Findings. | 12-13 |
| Issues in Oracle Internal Controls Manager | 12-14 |
| Correction Requests in Oracle Internal Controls Manager | 12-15 |
| Security for Issue Management Entities | 12-16 |
| Creating New Issue Management Entities | 12-16 |
| Profile based access to Issue Management Entities | 12-16 |
| Assignee based access to Issue Management Entities | 12-17 |
| Role based access to Issue Management Entities | 12-18 |

13 Control Reports

| | |
|---------------------------------------|------|
| Introduction | 13-1 |
| Risks with no Controls report. | 13-2 |

| | |
|---|------|
| Controls without Audit Procedures report | 13-2 |
| Controls with no Risks report. | 13-3 |
| Risk Control Matrix report | 13-3 |
| Business Process Summary report | 13-5 |
| Process Organization Summary report. | 13-5 |
| Audit Procedures Summary report | 13-6 |
| 14 Extensible Attributes | |
| Introduction | 14-1 |
| Enabled Objects. | 14-1 |
| Setup of Extensible Attributes | 14-3 |
| Recording Extensible Attributes | 14-5 |
| 15 Roles and Privileges in Oracle Internal Controls Manager | |
| Introduction to Security in Oracle Internal Controls Manager | 15-1 |
| Function Security. | 15-1 |
| Data Security | 15-1 |
| Data Security Details | 15-2 |
| Prerequisite | 15-2 |
| Organizations | 15-3 |
| Organization Processes | 15-5 |
| Risk Library Processes | 15-6 |
| Audit Engagements | 15-8 |
| 16 Function Security in Oracle Internal Controls Manager | |
| Introduction | 16-1 |
| Processes in Oracle Internal Controls Manager | 16-2 |
| Controls in Oracle Internal Controls Manager | 16-3 |
| Audit Procedures in Oracle Internal Controls Manager | 16-4 |
| Risks in Oracle Internal Controls Manager | 16-4 |
| Audit Project Evaluations in Oracle Internal Controls Manager. | 16-5 |
| Process Certifications in Oracle Internal Controls Manager | 16-6 |
| Financial Statement Certifications in Oracle Internal Controls Manager | 16-7 |
| Issue Management in Oracle Internal Controls Manager. | 16-8 |
| 17 Introduction to Application Controls Monitoring | |
| Introduction | 17-1 |
| Introduction to Application Controls Monitoring and Governance | 17-1 |
| Overview of the Application Controls Monitoring feature | 17-2 |
| Application Controls in the Oracle E-Business Suite. | 17-2 |
| Application Controls Management using the OICM Application Controls Monitoring feature | 17-3 |
| IT Audit Execution | 17-4 |
| Evaluate the Complexity of IT Processes. | 17-5 |

| | |
|--|------|
| Scope the IT Audit Project | 17-5 |
| Evaluate the IT Control System | 17-5 |
| Application Controls Monitoring in the Audit Cycle | 17-5 |

18 Setup of Application Controls Management

| | |
|---|-------|
| Introduction | 18-1 |
| Definitions | 18-1 |
| Application Controls Monitoring Architecture | 18-2 |
| Setting Up Application Controls Management | 18-3 |
| Prerequisites. | 18-3 |
| Setup Groups | 18-3 |
| Setup Parameters. | 18-5 |
| Reporting Groups | 18-8 |
| Remote Application Instances | 18-9 |
| Note on Processing Business Events | 18-11 |

19 Administer Application Controls Management

| | |
|--|------|
| Introduction | 19-1 |
| Using Application Controls Monitoring | 19-1 |

20 Application Controls Monitoring Implementation Checklist

| | |
|----------------------------------|------|
| Introduction | 20-1 |
| Checklist Steps | 20-1 |

21 Seeded Setup Groups and Parameters

| | |
|---|-------|
| Introduction | 21-1 |
| Setup Group Detail Listings | 21-1 |
| Setup Group Name: Financials Options | 21-1 |
| Setup Group Name: Payables Options | 21-3 |
| Setup Group: Receivables Options | 21-6 |
| Setup Group Name: Cash Parameters. | 21-9 |
| Setup Group Name: Set of Books | 21-10 |
| Setup Group Name: Tax Options | 21-11 |
| Setup Group Name: Inventory Parameters. | 21-12 |
| Setup Group Name: Purchasing Options | 21-14 |
| Setup Group Name: Receiving Options | 21-16 |
| Setup Group Name: Shipping Parameters | 21-17 |
| Setup Group Name: Assets System Controls | 21-18 |
| Setup Group Name: Federal Options | 21-19 |
| Setup Group Name: Federal System Parameters | 21-19 |

Send Us Your Comments

Oracle Internal Controls Manager Implementation Guide, Release 11i

Part No. B12267-04

Oracle welcomes your comments and suggestions on the quality and usefulness of this publication. Your input is an important part of the information used for revision.

- Did you find any errors?
- Is the information clearly presented?
- Do you need more information? If so, where?
- Are the examples correct? Do you need more examples?
- What features did you like most about this manual?

If you find any errors or have any other suggestions for improvement, please indicate the title and part number of the documentation and the chapter, section, and page number (if available). You can send comments to us in the following ways:

- Electronic mail: appsdoc_us@oracle.com
- FAX: 650-506-7200 Attn: Oracle Financials Documentation Manager
- Postal service:
Oracle Financials Documentation Manager
Oracle Corporation
500 Oracle Parkway
Redwood Shores, CA 94065
USA

If you would like a reply, please give your name, address, telephone number, and electronic mail address (optional).

If you have problems with the software, please contact your local Oracle Support Services.

Preface

Intended Audience

Welcome to Release 11i of the *Oracle Internal Controls Manager Implementation Guide*.
See Related Documents on page xii for more Oracle Applications product information.

TTY Access to Oracle Support Services

Oracle provides dedicated Text Telephone (TTY) access to Oracle Support Services within the United States of America 24 hours a day, seven days a week. For TTY support, call 800.446.2398.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible, with good usability, to the disabled community. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at <http://www.oracle.com/accessibility/>.

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

Structure

- 1 Introduction to Oracle Internal Controls Manager
- 2 Processes and Organizations in Oracle Internal Controls Manager
- 3 Process Approvals & Change Management

- 4 Risks and Controls in Oracle Internal Controls Manager**
- 5 Audit Procedures in Internal Controls Manager**
- 6 Risk Library Change Control**
- 7 Assessments in Oracle Internal Controls Manager**
- 8 Audit Engagements**
- 9 Segregation of Duty Constraints**
- 10 Process and Organization Certification**
- 11 Financial Statement Certification**
- 12 Findings in Oracle Internal Controls Manager**
- 13 Control Reports**
- 14 Extensible Attributes**
- 15 Roles and Privileges in Oracle Internal Controls Manager**
- 16 Function Security in Oracle Internal Controls Manager**
- 17 Introduction to Application Controls Monitoring**
- 18 Setup of Application Controls Management**
- 19 Administer Application Controls Management**
- 20 Application Controls Monitoring Implementation Checklist**
- 21 Seeded Setup Groups and Parameters**

Related Documents

Do Not Use Database Tools to Modify Oracle Applications Data

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

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

Because Oracle Applications tables are interrelated, any change you make using an Oracle Applications form can update many tables at once. But when you modify Oracle Applications data using anything other than Oracle Applications, you may change a row in one table without making corresponding changes in related tables. If your tables get out of synchronization with each other, you risk retrieving erroneous information and you risk unpredictable results throughout Oracle Applications.

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

Introduction to Oracle Internal Controls Manager

This chapter covers the following topics:

- Introduction
- Corporate Governance
- Overview of Oracle Internal Controls Manager
- Setup of Oracle Internal Controls Manager
- Application Controls Monitoring
- Integration with E-Business Suite Applications
- Responsibilities in Oracle Internal Controls Manager

Introduction

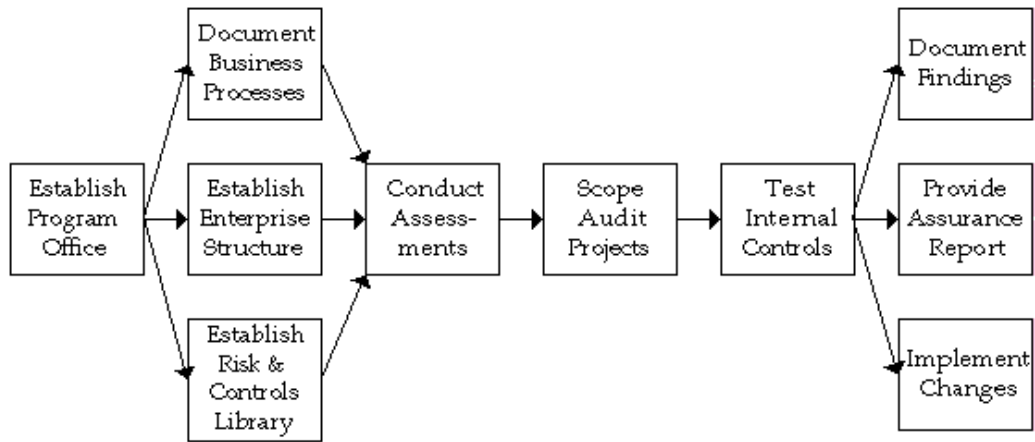
Oracle Internal Controls Manager is a comprehensive tool for executives, controllers, internal audit departments, and public accounting firms to document and test internal controls and monitor ongoing compliance. It is based on COSO (Committee of Sponsoring Organizations) standards.

In many countries, governmental regulations apply to the testing and reporting of corporate internal controls. For example, in the United States, the Sarbanes-Oxley Act of 2002 makes reporting on a company's internal control mandatory for both management and external auditors.

This chapter provides an introduction to corporate governance and the Oracle Internal Controls Manager.

Corporate Governance

The following diagram provides a high level overview of a generic corporate governance business flow:



As shown in the above figure, corporate governance generally includes a series of tasks that must be performed in any organization.

Establish a Program Office

The program office is typically authorized by the most senior executives in the enterprise. The program office establishes internal and external oversight responsibility and sets the parameters under which other offices will operate. These parameters will include the dates and milestones by when internal controls need to be in place as well as the personnel in the organization whose involvement is critical for compliance. Specific Audit Engagements can be undertaken either as a scheduled activity or as the result of trigger events.

A critical task of the program office is to establish a framework that will be used to assess and manage the entity's risk as well as the controls mitigating that risk. The COSO framework is the most prevalent framework for assessing the effectiveness of an organization's internal controls.

Establish Enterprise Structure

Establish an organization structure that allows segregation of duties and alerts management of possible infringements. This exercise will also result in identifying specific departments that must be analyzed for compliance.

Document Business Processes

Identify and analyze all the business processes that are specific to a particular entity within the enterprise. A review of the entity's procedure manuals, interviews, and replicating existing procedures will often highlight the business processes involved. These processes must also be mapped to key financial accounts to provide reasonable assurance regarding the reliability of financial statements.

Establish a Risk and Controls Library

Create a library of all the recurring risks to which business process within the entity are exposed. To create this risk library auditors must take factors such as the business structure and control environment into consideration. Though some

financial, operational, and disclosure risks are specific to an entity, a business process is typically subject to the following types of risk:

- Recorded transactions are valid. For example, sales are for shipments made to non fictitious customers.
- Transactions are authorized. For example, payments are made for approved orders.
- Transactions are correctly valued. For example, sales are recorded for the correct amount of goods shipped.
- Transactions are properly classified. For example sales transactions are included in the correct accounts and properly summarized.
- Transactions are recorded at the proper time. For example, sales are recorded on a timely basis.
- Transaction are free from omissions and mistakes. For example, all sales that have taken place are recorded.

The library also consists of internal controls set up to mitigate process risk. Analyze the internal controls of the entity that are currently in place and add them to the controls library.

Control procedures generally fall into the following five categories:

- Adequate separation of duties
- Maintaining an audit trail through adequate documents and records
- Procedures for authorization
- Control over assets and records
- Independent checks on performance

Auditors often create a matrix that links an entity's financial, operational, and disclosure risk to the internal controls currently in place. Where necessary, propose new internal controls or modify existing controls to mitigate risk.

Conduct Assessments

Once an auditor has obtained an overview of the design and operation of the internal control structure (through an investigation of processes, risks, and controls), an assessment of control risk must be made. This assessment will determine the extent of audit work that must be performed to test internal controls.

The assessment of control risk is usually conducted by detailed control objective for each major type of transaction. This will include collecting data for key processes such as:

- Acquisition and payment
- Sales and collection
- Production & inventory
- Processes related to employees
- Capital acquisition, depreciation, and repayment
- Processes related to debt and investment portfolios

While making assessments, it is also critical that you monitor issues from whistle blowers. These can be suppliers, customers & employees. Periodically, a survey can

be conducted for concerned stakeholders to obtain their opinion on the adequacy of internal controls.

Finally, document the results of your assessment evaluations.

Scope Audit Engagements

Identify the nature of the audit project, the scope of testing, and the resources required.

Test Internal Controls

As a prerequisite to testing, it is important to define key metrics for evaluating internal controls. Audit procedures can then be designed to test whether internal controls are effective and operating as designed. Ensure that the internal controls are being tested on a sample that is representative of the population.

Document Results and Provide Audit Opinions and Reports

Document all audit procedures and their results. Based on these results, auditors issue opinions and reports. It is useful to integrate results and alerts into the disclosure and reporting cycle.

Evaluations and results must be communicated to the audit committee and independent auditor regarding issues such as the following:

- Control Deficiencies
- Fraud
- Material Weaknesses

Implement Changes

Based on the audit results, you can propose new internal controls or modify existing controls to improve their effectiveness in mitigating risk.

Overview of Oracle Internal Controls Manager

As a key module of Oracle's Internal Control Applications, Oracle Internal Control Manager is a comprehensive audit tool that offers web based risk and audit management features. The module can be used by executives, controllers, internal audit departments, and public accounting firms to document and test internal controls and monitor ongoing compliance.

With Oracle Internal Controls Manager, your company can increase internal control testing efficiency, improve risk assessment confidence, and lower external audit verification costs. Use the application's intuitive workbench to organize, execute, and manage audit activities like the following:

- Define standard business processes
- Set up risks to which processes are exposed
- Set up controls that can mitigate process risk
- Set up the Organization Structure (Auditable Units) and map processes to this structure

- Record your assessment of the organization's compliance with established controls and regulations
- Create audit procedures to verify controls
- Review the compliance of your business processes/systems and record audit results.

Setup of Oracle Internal Controls Manager

The following sections provides a brief overview of the tasks that must be undertaken to set up and execute audits using the Oracle Internal Controls Manager application.

Define Standard Business Processes

Use Oracle Internal Controls Manager to create processes that accurately reflect your enterprise's business flows. Processes can be authored using Oracle Tutor (preferred) or Oracle Workflow, both of which integrate with Oracle Internal Controls Manager.

Note: For more details, refer to Processes and Organizations in Oracle Internal Controls Manager, page 2-1 and Business Process Change Management, page 3-1

Set Up a Risk and Controls Library

The risk library consists of processes and risks, as well as the policies, procedures, and activities that allow an organization to address those risks.

Risks: Use Oracle Internal Controls Manager to create and maintain a library of reusable risks that can then be associated with business process in the organization.

Controls: Set up controls that can mitigate process risk.

Risk libraries can consist of content from external sources. If you decide to implement a partner's library, Oracle Internal Controls Manager includes a spreadsheet interface that allows third party content to be imported.

To maintain the integrity of information within the risk library, creation or modification of library items in Oracle Internal Controls Manager is controlled by an approval process.

Note: For more details, refer to:

Risks and Controls, page 4-1

Audit Procedures, page 5-1

Risk Library Change Control., page 6-1

Set up the Organization Structure (Auditable Units) and map processes to this structure

The entire setup of Oracle Internal Controls Manager is done within the context of "Auditable Units." An Auditable Unit is a special category of an Oracle organization.

Note: For more details, refer to Processes and Organizations in Oracle Internal Controls Manager., page 2-1

Record Your Assessment of the Organization's Compliance with Established Controls and Regulations

With respect to testing controls, as well as other tests like tests of details of balances, the amount of procedural work performed in an audit depends to a large extent on an auditor's assessment of the organization's internal control structure and compliance with established controls and regulations.

Oracle Internal Controls Manager enables you to incorporate an assessment of the organization regarding its internal control structure and compliance. The assessment is made with respect to:

- Predefined components affecting the organization's audit environment
- A particular organizational context

Note: For more details, refer to Assessments in Oracle Internal Controls Manager., page 7-1

Create Audit Procedures to Verify Controls

Audit procedures provide detailed steps to be performed during audit fieldwork. They are designed to achieve specific audit objectives by validating the effectiveness of controls, in terms of their design, as well as their operation. In Oracle Internal Controls Manager, you can create audit procedures and associate them with the controls that the procedures are supposed to verify.

Note: For more details, refer to Audit Procedures in Internal Controls Manager, page 5-1.

Set up Audit Engagements to Manage Audit Assignments

Internal audits in organizations are usually managed as projects and audit procedures typically translate into tasks within these projects. Once you have reviewed compliance and completed the audit, Oracle Internal Controls Manager enables you to record your evaluations and audit opinions.

Note: For more details, refer to Audit Engagements in Oracle Internal Controls Manager., page 8-1

Test for Segregation of Duties Violations

Oracle Internal Controls Manager enables you to identify any combination of tasks in an enterprise as incompatible. Access to more than one task from a set of such tasks allows a user the opportunity for misconduct. An individual in the enterprise with access to more than one of these tasks is therefore in violation of a segregation of duties standard.

The application enables the proactive monitoring of incompatible tasks and reports those occurrences where a single person has access to them.

Note: For more details, refer to Segregation of Duty Constraints., page 9-1

Set up Business Process Certifications

Process certification requires process owners to provide assurance that their organization's processes are in compliance with the standard(s) utilized as the basis of

the firm's management system. It includes a series of rigorous audits and other activities to provide assurance that the organization's processes are adequate and effective.

Successful completion of an audit and any related follow-up activities which may be required results in the process being "certified." The certification attests to the process meeting the requirements of the applicable standard. External auditors seek objective evidence of such a system being established and effectively implemented prior to issuance of financial statements.

Oracle Internal Controls Manager provides an elaborate mechanism to certify your business processes. You can use the results of Audit Engagements executed in the application as a basis for the certification.

Note: For more details, refer to Process Certification., page 10-1

Set up Financial Statement Certifications

The financial audit is conducted to determine whether a firm's financial statements are in compliance with specified criteria, typically generally accepted accounting principles. Oracle Internal Controls Manager enables you to use audit evaluations and process certifications to certify your financial statements.

Note: For more details, refer to Financial Statement Certification., page 11-1

Record, Track, and Resolve Findings

During the audit process, non-conformities to established standards are often discovered and these anomalies are identified as "Findings." They are typically items of material concern that violate sound accounting practice and accountability.

A certification cannot be issued until all Findings are effectively addressed and remedied. Oracle Internal Controls Manager allows you to record and track Findings that come to light during the execution of your Audit Engagements.

Note: For more details, refer to Findings in Oracle Internal Controls Manager., page 12-1

Run Control Reports

The application provides seven predefined risk library reports that enable you to periodically verify the accuracy and integrity of the processes and objects that are present in your risk library.

Note: Reports in the Oracle Internal Controls Manager are discussed in detail under Control Reports., page 13-1

The following sections apply across the application:

Setup Extensible Attributes

Users interact with a variety of risk library objects while monitoring ongoing compliance using Oracle Internal Controls Manager. It is necessary and useful to capture and track additional and unique data associated with these objects. The application provides you with this ability in the form of Extensible Attributes.

These are user defined attributes that serve to capture additional information associated with risk library objects. Entries for these attributes can be validated against predefined value sets.

Note: For more details, refer to Extensible Attributes in Oracle Internal Controls Manager, page 14-1

Setup Roles and Privileges

Security in the application is implemented through both

- Function Security (described in the next section)
- Data Security

Data security is at a lower level than function security in that users having access to the same function can view different data sets based on their data access rights. The concept is based on providing access privileges on instances of objects (like processes) to specific users or user groups.

Privileges can be grouped together into an assigned "Role." Oracle Internal Controls Manager seeds a variety of roles corresponding to the object.

Note: For more details, refer to Roles and Privileges in Oracle Internal Controls Manager, page 15-1

Set up Function Security

The Oracle E-Business suite Architecture provides the ability to identify pieces of application logic as functions. The applications system administrator then administers function security by creating responsibilities that include or exclude particular functions.

Oracle Internal Controls Manager provides function security in select windows of the application.

Note: For more details, refer to Function Security in Oracle Internal Controls Manager, page 16-1

The following sections refer to the **Applications Controls Monitoring** feature in Oracle Internal Controls Manager.

Application Controls Monitoring

Introduction to Application Controls Monitoring and Governance

The accuracy and reliability of a firm's business processes and financial reporting are to a great extent dependent on the reliability and functioning of its IT systems and control environment. To meet the ongoing demands of assessing the IT control environment and minimize the cost of compliance, IT departments need an automated approach for monitoring and testing IT controls.

The Application Controls Monitoring feature enables companies to effectively and efficiently manage their IT environment by monitoring IT controls within the Oracle E-Business Suite. The application supports a number of high level control objectives within the CobiT framework such as maintaining application software, managing changes, ensuring systems security, and managing configuration.

Note: Also refer to the chapter Introduction to Application Controls Monitoring and Governance , page 17-1

Setup the Application Controls Management feature

Before Application Controls Monitoring can be used to report on changes in application controls, it must be implemented appropriately.

Note: For more details, refer to Setup of Application Controls Management., page 18-1

Administer Application Controls Management

Once the definition of Application Controls Monitoring is complete, you can use the application to query setup changes in your data. Application Controls Monitoring allows you to search for application control values and changes in those values using primarily four criteria:

- Reporting Group
- Application
- User
- Instance

Note: For more details, refer to Administer Application Controls Management., page 19-1

Application Controls Monitoring Implementation Checklist

When you install Oracle Internal Controls Manager, the installation process automatically creates the responsibility "IT Auditor." This responsibility includes the necessary functions to setup and implement the application. Hence as a prerequisite step, setup the appropriate users by assigning them this responsibility for the implementation.

Note: For a checklist of tasks that must be executed to complete the implementation of the Application Controls Monitoring feature, refer to Application Controls Monitoring Checklist, page 20-1.

Seeded Setup Groups and Parameters

The Application Controls Management feature enables IT managers and auditors to track changes to Setup Parameters in several modules within the Oracle E-Business Suite.

This chapter provides a detailed listing of the specific Setup Groups, Applications, and Setup Parameters that can be audited for changes.

Note: For more details, refer to Seeded Setup Groups and Parameters., page 21-1

Integration with E-Business Suite Applications

Oracle Internal Controls Manager is independent of the applications that it tests and validates and can be successfully deployed in any environment (Oracle or non Oracle). However, integration with other modules in the Oracle E-Business suite provides additional benefits as described below.

Oracle Tutor: Oracle Tutor is a powerful application for mapping and documenting your business processes and workflows. It offers procedure authoring, automatic flowcharting, and role based publishing. Oracle Tutor also contains predefined business models and flows.

Business processes authored in Tutor can be uploaded into Oracle Internal Controls Manager. The import automatically creates the same processes in Oracle Internal Controls Manager along with a visual diagram of the process flow. Oracle Tutor is the preferred tool for procedure authoring and documentation.

Oracle Workflow: Oracle Workflow charts your processes through the E-Business suite, controlling and enforcing the flows that work for your business. It is an active work management tool and serves as the database of business processes and process activities.

Business workflows defined in the Oracle Workflow Builder can be made available as processes in Oracle Internal Controls Manager. You therefore ensure that the process is executed in the way that you set it up.

Oracle Files: Oracle Files is a document management tool. Help files and process documentation developed using Oracle Tutor or any other tool can be associated with procedures and applicable processes. Process documentation often becomes the basis for compliance checking performed by auditors.

Oracle Files provides you with document version control, check in, check out, and storage in an Oracle Database.

Oracle Scripting: Oracle Scripting is a powerful tool for quickly building questionnaires, easily identifying survey participants, deploying the surveys via e-mail, and allowing respondents to fill out questionnaires via the internet.

By obtaining employee and stakeholder feedback on processes and internal controls, Oracle Scripting helps you to provide an effective control environment and perform high level risk assessments. Use the survey results to help in assessing the extent of audit work to be performed.

Once seeded, survey scripts can be deployed and used with minimal changes. You can review a seeded survey, make organization specific changes, and then redeploy them to collect information from survey participants.

Oracle Corporate Performance Management: Enterprise performance management encompasses activities like:

- Strategic goal setting and alignment
- Planning, budgeting, forecasting and modeling
- Operational analytics and reporting

Several Oracle products make up the Corporate Performance Management framework. These include applications like Oracle Financial Analyzer, Sales Analyzer and Performance Analyzer, Oracle Activity Based Management, Oracle Balanced Scorecard, and Oracle Daily Business Intelligence.

By setting process control limits within these applications, the performance management framework allows you to constantly monitor your business processes and notify you of exceptions that may warrant audit work.

Oracle Project Applications: By creating your audit procedures as projects set up in Oracle Projects, you get all the benefits of the Oracle Projects family of applications. These applications include

- Oracle Project Management
- Oracle Project Costing
- Oracle Project Resource Management
- Oracle Project Collaboration
- Oracle Project Intelligence

Oracle Approvals Management: The integration with Oracle Approvals Management enables a formal approval of risks, controls, and audit procedures. Approval is required for the creation and modification of these risk library objects. There is no requirement to customize any application code.

These rules are setup in Oracle Approvals Management and determine who must approve a risk library object before it can be used. Approvers can be one or more individuals in a hierarchy.

Other Oracle E-Business Suite modules: If your environment includes Oracle E-Business suite applications like Oracle Payables, Oracle Receivables, etc., several internal controls in those modules are made available to Oracle Internal Controls Manager by Oracle development.

Note: For more information, refer to Automation Type, Application, and Control Source, page 4-13.

To enable the certification of financial statements, accounts within FSG Reports are automatically made available to Oracle Internal Controls Manager. Financial Statement Generator (FSG) is a powerful ad hoc reporting tool and is a component of the Oracle General Ledger module.

Responsibilities in Oracle Internal Controls Manager

The Oracle Internal Controls Manager is pre-seeded with several responsibilities that are used to access the application. The following tables provide more details on these responsibilities.

The table below lists the Oracle Internal Controls Manager responsibilities along with their contextual details and relevant chapters:

| Name of Pre-seeded Responsibility | Contextual Information | Chapter |
|--|---|------------------------------|
| Internal Controls Manager Super User (SSW) | Business Processes, Risk and Controls Library, Assessments | Chapters 2 - 6, 14 - 16 |
| Internal Controls Manager Super User (Forms) | Oracle Internal Controls Manager related Profiles and Lookups | All relevant setups |
| Internal Auditor | Assessments, Audit Engagements, Segregation of Duty Violations, Findings and Remediations | Chapters 7, 8, 9, 12 14 - 16 |
| Business Process Owner | Process Variations and Exceptions, Process Certifications, Issues and Remediations | Chapters 10, 12, 14 - 16 |
| Global Operations Controller | Process Certifications, Issues and Remediations | Chapters 10, 12, 14 - 16 |
| Signing Officer | Financial Statement Certification, Issues and Remediations | Chapters 11, 12, 14 - 16 |
| Oracle ICM Discoverer Reports | Control Reports | Chapter 13 |
| IT Auditor | Application Controls Monitoring | Chapters 17 - 21 |

Note: For more details on security within Oracle Internal Controls Manager, refer to Roles and Privileges in Oracle Internal Controls Manager, page 15-1 and Function Security in Oracle Internal Controls Manager, page 16-1.

The following table displays a matrix of responsibilities and menu items in Oracle Internal Controls Manager:

| MENU ITEMS | Global Operations Controller | Business Process Owner | Signing Officer | Internal Auditor | Oracle Internal Controls Manager Super user | Library Manager |
|-------------------------------|-------------------------------------|-------------------------------|------------------------|-------------------------|--|------------------------|
| Create Process Certifications | x | | | | | |
| Review Process Certifications | x | | | | | |
| Certify Processes | x | x | | | | |
| Create and Track Issues | x | x | | | | |

| MENU ITEMS | Global Operations Controller | Business Process Owner | Signing Officer | Internal Auditor | Oracle Internal Controls Manager Super user | Library Manager |
|--|---|---------------------------------------|----------------------------|-----------------------------|--|----------------------------|
| Create and Track Remediation Actions | x | x | | | | |
| View "My Processes" | | x | | | | |
| View Certifications created by GPO | | x | | | | |
| Certify Financial Statements | | | x | | | |
| Create Financial Statement Certifications | | | x | | | |
| Track Issues created by Process Owners | | | x | | | |
| View Audit Evaluations | | | x | | | |
| View Org specific Process hierarchy | | | x | | | |
| View Process Certifications | | | x | | | |
| Create & Track Remediation Actions | | | x | x | | |
| Conduct Segregation of Duties Violation checks | | | | x | | |
| Create & Track Findings | | | | x | | |
| Record Evaluations | | | | x | | |

| MENU ITEMS | Global Operations Controller | Business Process Owner | Signing Officer | Internal Auditor | Oracle Internal Controls Manager Super user | Library Manager |
|--|---|---------------------------------------|----------------------------|-----------------------------|--|----------------------------|
| Scope Audit Engagements | | | | x | | |
| Conduct Assessments | | | | x | x | |
| Manage Risk Library | | | | x | x | x |
| Plan Organization specific process hierarchy | | | | x | x | x |
| Manage Setups | x | x | x | x | x | x |

Processes and Organizations in Oracle Internal Controls Manager

This chapter covers the following topics:

- Introduction
- Overview of Process Setups in Oracle Internal Controls Manager
- Creating Processes directly within Oracle Internal Controls Manager
- Importing Process Documents using Oracle Tutor
- Importing Processes using Oracle Workflow
- Importing Processes using Web ADI
- Process Objectives
- Process Attributes
- Associating Documents with Processes
- Linking Key Accounts with Processes
- Organizations in Oracle Internal Controls Manager

Introduction

A significant portion of the typical internal audit function is associated with the business processes in an enterprise. In addition, auditing standards referenced by most regulatory institutions define internal controls in the context of business processes.

Your first task in setting up Oracle Internal Controls Manager (OICM) is to create processes that accurately reflect your enterprise's business flows.

Overview of Process Setups in Oracle Internal Controls Manager

The following steps list the tasks you must complete to accurately create your processes in OICM.

1. Obtain an understanding of the business processes occurring within the enterprise by:
 - Reviewing documentation of current business processes
 - Interviewing business process owners

- Reviewing standard business flows within the organization
2. "Author" your processes in OICM using one of the four methods listed below:
- Create processes within the OICM application itself
 - Import processes using Oracle WebADI.
 - You can also bring in processes created in Oracle Tutor (preferred) or Oracle Workflow, both of which integrate seamlessly with OICM.

Process authoring consists of documenting the business processes for an organization. The documented processes are then used for assessing the organization's control environment through an identification of the risks and controls associated with the process. Since most business processes are hierarchical in structure, a process can be documented at several levels and can contain other processes.

Typically, the process owners and their designees do the authoring. Once the documentation is completed, the documented processes can be uploaded into the Internal Controls Manager process library. For processes authored in Oracle Tutor, a graphic image of the process flow can also be displayed to help users visualize the process.

Note that processes from different sources can be integrated together in a hierarchy in OICM.

Note: Each of these authoring methods is discussed in detail later in this chapter. Also refer to the *Oracle Tutor Author User Manual* and the *Oracle Workflow User's Guide*.

Once created, OICM allows you to enrich the definition of the process by identifying process attributes like process owner, process category, approval status, etc.

Note: For more information, refer to the section Process Attributes, page 2-19.

3. Associate procedure documents with OICM processes.

As part of the audit function, the internal auditor needs to document the business processes within an organization. You can associate these documents with the corresponding processes in OICM.

Oracle Tutor includes a repository of Oracle E-Business Suite procedural content that can be dynamically adapted to your company's unique business processes. With Oracle Tutor, you can author and publish procedural documentation that can be associated with processes in OICM.

Note: For more information, refer to Associating Documents with Processes, page 2-22.

4. Link key financial accounts with OICM processes.

Auditing standards require internal controls to provide reasonable assurance regarding the reliability of financial reporting.

By providing a link with general ledger accounts, OICM enables the integration between processes and the elements of financial statements. OICM allows you to associate each process with multiple financial statement accounts. For example, the Order to Cash process affects the Revenue, Deferred Revenue, Cost of Goods Sold, Finished Goods Inventory, and Accounts Receivable Control accounts.

Since processes are exposed to business risk, the association of key accounts with processes also establishes the link between financial statements items and the risks that they are exposed to. For example, the risk "customer default" would impact the financial statement item "Revenue" through the "Order-To-Cash" process.

Note: For more information, refer to Linking Key Accounts with Processes, page 2-25.

5. Load Risks, Controls, and Audit Procedures into the risk library and then associate them with your business processes.

Before they can issue audit opinions and compliance reports, auditors need to first execute appropriate audit procedures. These procedures verify the internal controls that have been set up to mitigate risks that the organization's business processes are exposed to.

Therefore risks, controls, and audit procedures must be associated with each other and with processes before an audit opinion can be issued.

Note: For more information on linking risks and controls with the processes in OICM, see Setting up Risks in Oracle Internal Controls Manager and Setting up Controls in Oracle Internal Controls Manager.

Note: For information on associating audit procedures with controls, see Setting up Audit Procedures in Oracle Internal Controls Manager.

6. Submit and approve Processes in OICM.

The verification of business processes which make up an organization is a major portion of the internal audit function. All processes and process revisions are created in a "Draft" status and must be approved before the process or its revision can be used in the system.

When processes are submitted for approval, notifications are sent to all concerned personnel (ex. process owners) and recipients of these notifications can review the process/ modified process prior to giving their approval.

Note: For more information, refer to Process Approvals and Change Management, page 3-1 in OICM.

The OICM application only allows users to view and modify processes that list them as the designated owner or otherwise have appropriate privileges on the process.

Note: For more information, refer to Roles and Privileges in Oracle Internal Controls Manager, page 15-1 and Function Security in Oracle Internal Controls Manager, page 16-1.

7. Map processes in OICM to the organization structure of the enterprise.

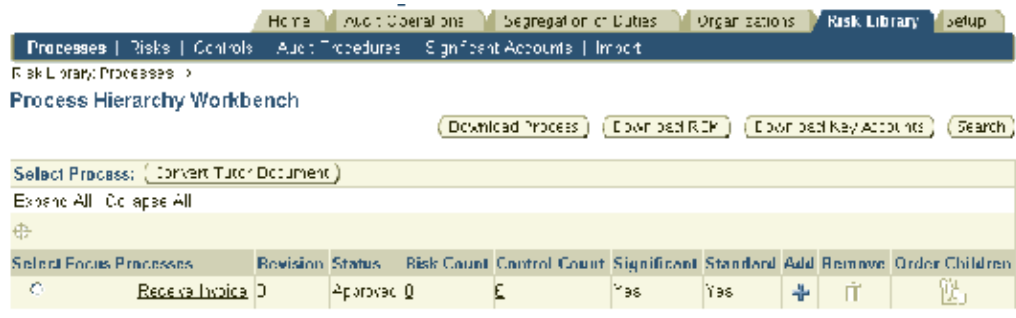
As different organizations may perform different processes, OICM allows you to associate specific processes with specific organizations in the enterprise. Note that an organization may be running a slight variation of a standard process. Such variations should be justified and subject to approval.

Note: For more information, refer to Organizations in Oracle Internal Controls Manager, page 2-29. For detailed information on setting up organizations, refer to *Using Oracle HRMS – The Fundamentals*.

Creating Processes directly within Oracle Internal Controls Manager

Processes can be created in the Risk Library as follows:

| Topic | Navigation Path |
|--|---|
| Creating Processes in the application Risk Library | <p>Using the Super User (or equivalent) responsibility, click the Risk Library tab and then the Processes subtab.</p> <p>Click the Modify icon for the appropriate process to create the new process as its child. To create a top level process, choose the Modify icon for the node "All Processes".</p> <p>In the Process Hierarchy Workbench, click the "Add" icon.</p> |



In the Add Process window, you select the option to "Author a New Process." The new process is created as a child to the selected process.

Process Code and Name

The screenshot shows the 'Enter Process Attributes' form. At the top, there are navigation tabs: Home, Audit Operations, Segregation of Duties, Organizations, Risk Library, and Setup. Below these are sub-tabs: Processes, Risks, Controls, Audit Environment, Significant Accounts, and Violation. The main title is 'Enter Process Attributes'. There are 'Cancel' and 'Apply' buttons. The form has several input fields: 'Process Code' with the value 'OICM_406', 'Display Name', 'Description', 'Process Type' (dropdown menu showing 'Process'), 'Process Category' (dropdown menu showing 'Routine'), 'Significant Process' (dropdown menu showing 'Yes'), and 'Classification' (dropdown menu). Below the form, there are tabs for 'Basic Information', 'Process Significance', 'Objectives', 'Significant Accounts', 'Process Controls', 'Violation', and 'Attachments'.

The application distinguishes the process name and code as follows:

Consider a process "Approve Purchase Order." This process may exist in multiple hierarchies and organizations and be associated with different risks, controls, etc. depending on the environment. Hence there is a need for multiple and different "Approve Purchase Order" processes to co-exist in the system.

OICM therefore supports multiple processes with the same name. The application qualifies each process internally with a unique Process Code and this is the unique identifier of the process. The Process Code can be user entered or system generated with a defined pre-fix.

Process Attributes

Subsequently complete the setup of the Process by entering its attributes.

Note: For detailed information, refer to Process Attributes, page 2-19.

Importing Process Documents using Oracle Tutor

Though not required for the implementation of OICM, Oracle Tutor is Oracle's preferred procedure authoring and documentation tool. Tutor provides a ready and comprehensive base of procedures that can be easily modified to match your business processes.

In addition, an out of the box integration between the two products enables a process that is authored in Oracle Tutor to be easily loaded into OICM. The import automatically creates the OICM processes along with visual diagrams of the process flow.

Note: For detailed information on creating and modifying process flows and procedures in Oracle Tutor, refer to the *Oracle Tutor Author User Manual*.

To Import Process Documents using Tutor

Perform the following tasks to import processes from Tutor into OICM:

1. Create your processes in Oracle Tutor.

- Turn on the Audit mode in Tutor Author Preferences by clicking on Author > Flowchart Preferences > Select Enable Audit Mode > OK.

This setting places the process (RE_XXXX) .fl1 files into the Audit folder. .fl1 is the file format that is readable by OICM and is used to populate the H-grid.

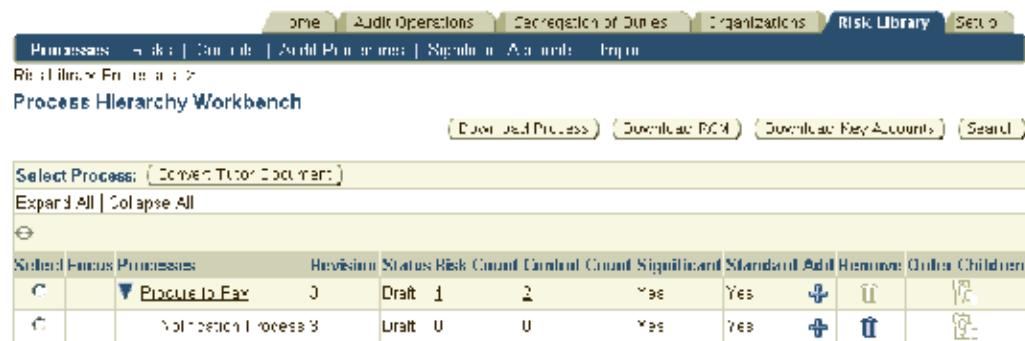
- From the Tutor/Word menu bar select Author > Flowchart.

This generates a flow chart for the process and also creates a (process name).fl1 file in the Tutor installed directory/Author/Audit.

- Verify that the corresponding .fl1 file is placed in the /Author/Audit folder.
- In the Risk Library > Process tab of OICM, select the radio button appropriate to the process that will serve as a parent process. The Tutor processes being imported will be created as children of this parent. Note that you can expand the processes shown by clicking on "Expand All."

The highest level parent in OICM is "All Processes." If there are no processes listed, create and import a parent process document, which will define all your high level processes.

We recommend that you initially load the highest level processes first (for example Procure to Pay, Order to Cash, etc.) and then load the sub processes in the order they are sequenced. A parent process can have many child processes associated with it.



- Click Convert Tutor Document. The Attach link shows existing attachments, if any.
 - By selecting Treat Tutor Processes as New, the application considers duplicate process names as new processes and does not replace those that exist.
 - If the Treat Tutor Processes as New is not checked and the process being added already exists, then the existing process is added as a child of the selected process. Note that if two existing processes have the same name as the process being added, the conversion will error out.
- Now click Add and provide the following:
 - A Description of the file that is being attached.
 - The Category of the attached file. For Tutor documents, this value is "ICM: Tutor Flow Chart Data."
 - Whether the Attachment Type is a File, URL, or a Text file. For Tutor files, select the "File" radio button and then click Browse. In the browse window go to the Oracle Tutor installed directory /Author/Audit and select the .FL1 file that is

associated to the process doc (the file name is the same except that it has a .FL1 extension).

Note: If you choose to upload a process flow diagram from Tutor at this time, click Add Another and follow the directions given in Step 4 of the section To Import Process Flow Diagrams using Tutor.

8. Finally complete importing the Tutor document as follows:
 - Click Finish to complete the addition of the file. The window shows a summary of attachments for the selected process or procedure.
 - Click Return to return to the Processes screen.
 - Click Apply to apply the changes.
 - Click Convert to load the new process. This launches a concurrent process with a request ID.
9. When the concurrent process has completed, you can view the imported processes in the Risk Library Window under the Processes tab.
10. If the changes are not visible, go to the Forms menu and find the concurrent request with the ID obtained above. If there is an error click the View Log and you should see the error message and log file.

Note on importing tasks at the lowest level

In a Tutor document, you can set up multiple levels of sub-processes / sub-tasks under a parent process or task. During the import, only "First Level" sub-processes or tasks in the Tutor document will be uploaded to OICM.

You can upload a subsequent level of sub-processes/sub-tasks under the prior level by selecting the appropriate parent process/task before executing the next import. In OICM, a parent process can have an unlimited number of child processes associated with it. You are also allowed unlimited levels of sub processes and sub-tasks under a parent level process.

In a large and complex environment, it is conceivable that the view of processes and tasks as seen in the Risk Library window can soon get overwhelming since each process or task appears as a separate entry (line). In such a context, we recommend that all lowest level tasks under a process that do not have risks and controls directly associated with them, be described in an attached HTML file. Note that lowest level tasks are typically in procedures or instruction documents.

Audit Mode Selection

As needed, you can flag tasks within Tutor processes or procedures with the appropriate Audit mode selection:

- Automatic Control
- Manual Control
- Both

Note: In Oracle Tutor, this flag is typically set at the lower level of procedures and instructions as opposed to tasks in higher level processes. See the *Oracle Tutor Author User Manual* for more information on flagging tasks using Audit Mode.

Process and tasks that are flagged with an Audit Mode in Oracle Tutor are automatically created in OICM with a:

- Process Type of Control Activity
- Control Activity Type of Automatic, Both, or Manual (depending on the Audit Mode)

Attaching a File to a Process

The steps to attach a file to a process are shown below.

1. In the Risk Library > Process tab of OICM, select the radio button for the process to which you want to attach your procedures document. This process will serve as the parent for the lowest level tasks.
2. Click Convert Tutor Document and then on Attach. The resulting window shows existing attachments, if any.
3. Now click Add Attachments and provide the following:
 - A Description of the file that is being attached.
 - For the Category of the attached file select "Miscellaneous."
 - Whether the Attachment Type is a File, URL, or a Text file. Make sure that your entry corresponds to the appropriate radio button in this window.
4. Finally complete importing the attachment as follows:
 - Click Finish to complete the addition of the file. The window shows a summary of attachments for the selected process or procedure.

- Click Return to return to the Processes screen.
 - Click Apply to apply the changes.
 - Do NOT click Convert as the HTML file (or any other file) is an attachment only. If you click this button, the concurrent process that is launched completes with errors.
5. You can now view the lowest level tasks by selecting the parent level process, clicking on Convert Tutor Document, and then selecting Attachments.
- Note:** Also refer to the section Associating Documents with Processes, page 2-22.

To Import Process Flow Diagrams using Tutor

Perform the following tasks to import process diagrams from Tutor into OICM:

1. From the Tutor/Word menu bar select Author > Convert To html. This generates a gif file depicting the flow of the process or procedure and stores the (process name).gif file in the Tutor installed directory. The Tutor installed directory is either /US/APPSHTML/FND or Tutor11i/HTML depending on the Tutor Author HTML option selected.
2. In the Home > Process tab of OICM, select the radio button corresponding to the process or procedure that the flow diagram represents. Note that you can expand the processes shown by clicking Expand All.
3. Click Convert Tutor Document and then Attach. The resulting window shows existing attachments, if any.
4. Now click Add Attachments and provide the following:
 - A Description of the gif file that is being attached.
 - The Category of the attached file. In this case, this value is "ICM: Flow Chart Diagram."
 - The Attachment Type. For Tutor GIF files, select the "File" radio button and then click Browse. In the browse window go to the Oracle Tutor installed directory and select the GIF file corresponding to the process or procedure.
5. Finally complete importing the flow diagram as follows:
 - Click Finish to complete the addition of the file. The window shows a summary of attachments for the selected process or procedure.
 - Click Return to return to the Processes screen.
 - Click Apply to apply the changes.
 - Click Convert to load the new process diagram.
6. You can view the imported process diagram by selecting the process in the Risk Library Window under the Processes tab.

Importing Processes using Oracle Workflow

Oracle Workflow provides a complete business process definition, automation, and integration solution. A workflow process consists of a sequence of activities that

together make up a business flow. The activities can include business events, automated functions, notifications to users, and sub-processes.

Using Oracle Workflow you can perform activities like the following:

- Define, implement, and enforce your organization's business policies
- Route information like approvals and data through the organization based on user defined rules
- Capture exceptions when they occur and take action based on the type of exception
- Integrate with trading partner systems

Workflows defined in the Oracle Workflow Builder can be made available as processes in OICM.

Benefits

- During the import of processes written in Oracle Tutor, only "First Level" sub processes or tasks in the Tutor document are uploaded to OICM. You need to upload a subsequent level of sub-processes / sub-tasks under the prior level by selecting the appropriate parent process/task before executing the next import.

This can be a disadvantage if you have several organizations with multiple levels of sub-processes/sub-tasks under a parent process or task. In a large and complex environment, it is conceivable that a large number of imports will be necessary to fully import your organization's processes.

On the other hand, processes defined appropriately in Oracle Workflow are automatically available in their entirety as processes in OICM. Sub-processes defined in Oracle Workflow under a particular parent process will be available as such in OICM.

- Oracle Workflow is an active work management tool. The Oracle platform hosts the business applications that are integrated with the Workflow Engine, the Business Event system, the Notification system, and directory services.

Hence by defining your business processes using Oracle Workflow Builder, you automatically ensure that the process is executed in the way that it is set up.

Note: For detailed information on using the Workflow Builder and workflow components and services, refer to the *Oracle Workflow Guide*.

It is important to note the following caveat with respect to Oracle Workflow: The setup of processes in Oracle Workflow Builder requires considerably more technical expertise than that required to create processes using Oracle Tutor.

To import processes using Oracle Workflow

The workflow processes that are imported can be of any ITEM TYPE. In Oracle Workflow, an Item Type is a grouping of workflow components into a high level category and all components of a workflow process (including the process itself) must be associated with a specific Item Type.

Pre-requisite

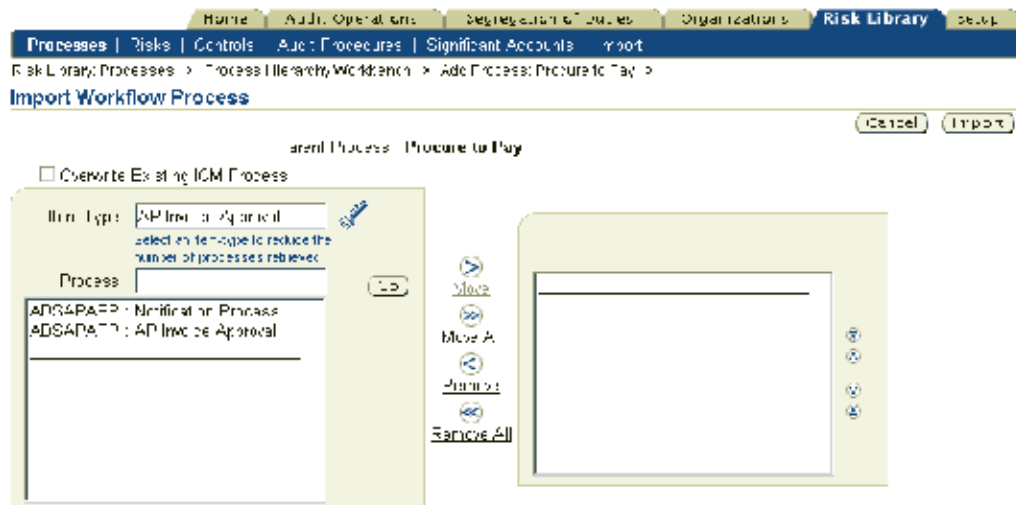
For processes written in the Workflow Builder to be available as processes in OICM, they must be defined under the "All Processes" node.

Steps in Workflow Builder

1. Open the Workflow Builder by clicking the Open icon (Ctrl-O).
2. Click the Database radio button. Enter user/passwd/SID.
3. A Shuttle box appears. On the left highlight the appropriate Item Type and click the left arrow to shuttle this item-type to the left box and then press OK.
4. Expand the Item Type and then expand Processes.
5. Double click on the process under which you want to create your processes.
6. Right Click with the mouse in the blank space that opens up and choose New Process. If this option is grayed out, then you do not have permission to create children for that process.
7. Enter process properties. Note that you can create as many processes as you need.
8. Now you need to create the activity transition data. Click on a node, for example Process1, right click, and draw the arrow to say Process2. This means Process2 follows Process1 in execution sequence.
9. Continue to create processes this way. Note that to be visible in OICM, the process that you create must exist under the ALL PROCESSES process (root). This is also seeded with the application.
10. Close the box and Save all Data.

Steps in Oracle Internal Controls Manager

| Topic | Navigation Path |
|--|--|
| Importing processes from Oracle Workflow | <p>Using the Super User (or equivalent) responsibility, click the Risk Library tab and then the Processes subtab.</p> <p>Click the Modify icon for the appropriate process to create the new process as its child. To create a top level process, choose the Modify icon for the node "All Processes".</p> <p>In the Process Hierarchy Workbench, click the "Add" icon and choose to "Import Processes from Workflow."</p> |



Once imported, process can be modified as appropriate in OICM. For example you can add children, risks, controls, etc. to the process.

Subsequent changes in the process within workflow are not automatically reflected in the OICM process. To later synchronize the OICM version with the Oracle Workflow copy, check the "Overwrite the Existing Process" option and re-import. This results in the OICM process matching the version from Workflow.

Note: The name and Item Type of the two versions of the process being imported from Workflow must be the same. If you choose to overwrite the existing process, then the Risk Library objects that are associated with the existing process will be deleted.

The imported Workflow process is a new revision and will not show up in the approved hierarchy until and unless approved.

Importing Processes using Web ADI

While conducting internal audits, companies build up libraries of significant business processes along with their associated risks and controls. Consulting firms have also created large data sets of risk library objects. These repositories are typically built over several years and incorporate the industry's best practices in executing processes and conducting audits.

Applications Desktop Integrator (ADI) is a spreadsheet based extension to the Oracle E-Business Suite and enables suite applications to import data using a native spreadsheet interface. With the import functionality in OICM, companies can leverage the existence of existing repositories by importing them from a file. The data can then be applied to their organizations with minimal customization.

OICM uses Oracle Web ADI for the import of all risk library objects
- processes, risks, controls, and audit procedures.

Note: For more information on importing risk and control objects into OICM, see Importing Risks and Controls into Oracle Internal Controls Manager. Also see Importing Audit Procedures into Oracle Internal Controls Manager.

To Import Processes using Web ADI

Processes constitute relatively static data and most organizations will typically import them infrequently.

| Topic | Navigation Path |
|--|---|
| Importing processes into OICM using WebADI | Using the Super User (or equivalent) responsibility, click the Risk Library tab and then the Import subtab. Select Viewer Settings and subsequently enter all required information into the import spreadsheet. Finally, select "Oracle-Upload" from the menu bar. |

Note the following points with regard to the import of processes using Oracle Web ADI.

- The process spreadsheet includes a parent process for every row on the spreadsheet. This allows you to import the entire hierarchy for the firm's business processes at the same time thereby eliminating the need for multiple uploads. The highest-level process is "All Processes."

By using the template correctly, you can not only define new processes (for example Sales Order Management), but also create an entire process hierarchy that looks like this:

All Processes
Order to Cash
Sales Order Management
Analyze to Agreement
- Attributes of processes are the major part of the spreadsheet and processes are imported/updated with these attributes. Validation of the import data is done within the spreadsheet itself through lists of values for all lookup based columns.
- Web ADI uploads the data from the spreadsheet into the AMW_PROCESSES_INTERFACE table. A concurrent program then uploads the data from the interface table to the base tables. You may choose to submit this program automatically during the upload. Any errors that occur during the import process are flagged as errors with appropriate error messages.
- Once data is imported, the profile option "AMW: Processes-Delete after import?" provides users with the option of deleting the rows from the interface. The default value is set to "Yes" so that once the rows are successfully imported, they are automatically deleted from the interface.
- AMW: Default Processes to Standard Process. This profile option lets users define if uploaded Processes should be defaulted as Standard Processes.

WebADI imports and Owner Privileges

The following logic applies to the process owner, finance owner, and application owner columns:

- Roles for the 3 owner columns (process owner, application owner, and finance owner) are not automatically granted for users in the import spreadsheet i.e. they are not synonymous with the column headers. Instead the following three site

level profile options will determine the privileges of users entered in the import spreadsheet as process, finance, and application owners.

1. AMW: Process Import Finance Owner column
2. AMW: Process Import Application Owner column
3. AMW: Process Import Process Owner column

These profile options can be set to any role within the process approvals domain. For example if the AMW: Process Import Process Owner column is set as "Process Reviewer", then user entered in the Process Owner column in the spreadsheet will only get a process reviewer role.

Note: For more information on roles available, refer to Roles and Privileges, page 15-1 in OICM.

- When importing new processes:

If user X is uploading a process P and specifies user Y in the Process Owner column, then Y is granted the "Process Owner" role. If User X does not specify a value in the Process Owner column, then no role is granted on the imported process to anyone.

Note: However, note the above caveat on site level profile options which effectively limits the role of the imported owners.

- When importing (updating) an existing Process:

Case 1: P has no process owners

If user X is updating a process P and specifies user Y in the Process Owner column, then Y is granted the "Process Owner" role.

Case 2: P has one specified process owner

Assume that the existing owner of process P is Q. If user X is updating P and specifies user Y in the Process Owner column, then Q is replaced by Y and Y is granted the "Process Owner" role.

Case 3: P has multiple process owners

Assume that process P has multiple process owners. If user X is updating P and specifies user Y in the Process Owner column, then Y is added as a "Process Owner" to the existing set of Process Owners of P.

Note: Again, note the above caveat on site level profile options which effectively limits the role of the imported owners.

- Additionally, the profile options "AMW: Access All Processes" is an instance set grant on all processes and is set at the user level. If this Profile Option is set to "Yes" for a particular user, then that user will have access to all processes in the instance.

The following table lists the fields in the body of the import spreadsheet:

| Field Name | Mandatory | Validation (Lookup Type) |
|-------------------------|-----------|--|
| Process Name | Yes | Free text / All valid process names in the system. |
| Process Code | No | Free text / All valid process codes in the system. |
| Parent Process Name | Yes | All valid process names in the system including "All Processes. Alternately, you can enter a new parent process name as free text. Since this process does not exist in the application tables, it must be entered and imported as a new process line in the spreadsheet. |
| Parent Process Code | No | Free text / All valid process codes in the system. |
| Process Owner | No | A valid Party in the AMW_EMPLOYEES_CURRENT_V view. |
| Finance Owner | No | A valid Party in the AMW_EMPLOYEES_CURRENT_V view. |
| Application Owner | No | A valid Party in the AMW_EMPLOYEES_CURRENT_V view. |
| Process Sequence Number | No | NA. This number determines the sequence in which the process appears in the hierarchy. |
| Revise/Delete Process | No | Revise/Delete |
| Approval Status | No | AMW_PROCESS_APPROVAL_STATUS |
| Process Category | No | AMW_PROCESS_CATEGORY |
| Significant Process | Yes | (Y/N) AMW_SIGNIFICANT_PROCESS |
| Standard Process | No | (Y/N) AMW_STANDARD_PROCESS |
| Standard Variation | No | All valid processes in the system |
| Process Type | No | All Valid Process Types |
| Control Activity Type | No | Automatic, Manual, Both |
| Attachment URL | No | NA |
| Classification | No | All valid Process Classifications |

Note: Standard Variation

If the process being uploaded is not a Standard Process, then the Standard Variation field MUST be entered i.e. the process being uploaded is a variation of the process entered in the Standard Variation field.

Note: Revise/Delete Process flag

During the import, processes are created if they do not exist and updated based on the status of the "Revise/Delete Process" flag. This flag supports process revisions as follows:

- The flag is ignored if the process does not exist.
- If the process exists and the flag is "Revise," the process will be revised if the process has an "Approved" status and updated if the process is in "Draft" status.
- If the process exists and the flag is "Delete," the process will be deleted. All sub processes in the hierarchy below this process will be deleted as well.

Profile Option Settings

The following profile option values need to be set correctly based on the load of the concurrent program.

1. BNE: Upload Retry Count

This indicates the number of times to check concurrent status. The default is 50.

2. BNE: Upload Sleep Seconds

This indicates the number of seconds to wait between each check of concurrent status. The default is 3. This indicates WebADI will wait for 150 seconds to finish the concurrent request.

3. "BNE: UNIX Physical Directory": should be set as file_path/cabo/

The file_path where the cabo directory is located.

4. The ICX profile "Apps Servlet Agent": should be set to "http://xxxxx:port/oa_servlets/"

Note that '/' is important at the end of the URL.

5. "BNE: Upload Staging Directory": should point to a directory where the apps user has write permission.

If not the user will get a write privilege error as follows:

IOException: Please have your system administrator view the bns.log file. Cause: java.io.FileNotFoundException:/Directory path/bnee0tdZvSg.xml (Permission denied) Action: Please contact your support representative.

The file "bnee0tdZvSg.xml" is dynamically generated and will vary with the concurrent program run.

Using Web ADI with Excel versions higher than Excel 2000

For Web ADI to work with these versions, perform the following three steps:

1. Open to the latest version of Excel
2. Go to Tools -> Macro -> Security -> Trusted Sources
3. Check the "Trust access to Visual Basic Project"

Process Objectives

All business processes, explicitly or implicitly, have objectives that the process is oriented towards. These objectives send a powerful signal as to what you intend to achieve by running the process in the organization. Process objectives are typically classified as being one or both of the following:

- Control objectives that must be met. For example, an Accounts Receivable department process may have control objectives that are consistent with segregating duties with respect to credit granting authority and sales commissions. Another control objective for this process could be ensuring authorized credit commitments.
- Performance objectives that the process must achieve. For example, the Accounts Receivable department process may have performance objectives that are consistent with minimizing working capital requirements, like "Days sales outstanding."

A review of your business process can help to determine these objectives. Once identified, process objectives provide guidance in identifying process risks as well as the controls to mitigate those risks. Process objectives, when used in conjunction with process definitions, can also provide useful benchmarks to process owners for evaluating the performance of their processes. To this end the application allows you to associate Key Performance Indicators with the process objective.

OICM allows you create objectives that can be associated with process definitions. The process objectives can be categorized as being control or performance objectives.

Setting up Process Objectives

OICM allows you to create process objectives in two ways:

- Manually set up your process objectives
- Import process objectives when importing risk library objects

Note that you can only define process objectives in the risk library of the OICM application.

Manually create process objectives

| Topic | Navigation Path |
|------------------------------------|---|
| Manually create process objectives | Using the Business Process Owner (or equivalent) responsibility, click the Setup tab and then the Risk Library subtab Select the (Process) Objectives Summary link under the Risk Library tab and then click the Create button |

1. Enter the attributes of the objective and specify whether it is a control or performance objective.

Risk Library

Audits

Findings

Financial Statements

Opinions

Import

Setup : Risk Library > Process Performance/Control Objectives Details

Process Performance/Control Objectives Details

Cancel

Save

* Objective Name

Minimize Bad Debt

Type

☒ Control Objective
 ☐ Performance Objective

Start Date

22-Jan-2004

End Date

30-Jan-2004

Defined By

Bacajun, Stanford

Objective Description

Performance Measures

| *Application Name | *Performance Measure Name |
|----------------------------|---------------------------|
| *Oracle Receivables | *AR Turnover |
| <div>Add Another Row</div> | |

For both control and performance objectives, you can associate a performance measure in the form of a Key Performance Indicator from the Oracle Daily Business Intelligence module. The same performance measure can be used by multiple objectives.

- Once the process objective is created, drill down to the Objectives section of the Process Details page

| Topic | Navigation Path |
|--|--|
| Link Process Objectives with Processes | <p>Using the Business Process Owner (or equivalent) responsibility, click the Risk Library tab and the Processes subtab.</p> <p>For the relevant process, click the Modify icon to access the Process Hierarchy Workbench. Drilldown into the appropriate process and select the Update dropdown.</p> <p>Select the Objectives subtab to add and/or update Process Objectives hyperlink.</p> |

Note: For detailed information on the Process Hierarchy Workbench, refer to Process Approvals and Change Management, page 3-1.

Import Process Objectives

Instead of creating process objectives manually and then associating them with processes individually, OICM furnishes a powerful import mechanism for process objectives. Using this functionality, you can import and associate process objectives with processes in a single step.

Note that process objectives cannot be imported while importing processes into the risk library. Instead process objectives form a part of the spreadsheet to import risks and controls. This is because these objectives can only be fully understood in the context of process risks. By virtue of orienting a process in a particular direction, process objectives expose processes to risk. Hence the import of process objectives is along with risks and controls in OICM.

Note: Processes must exist in the application before the import of risks, controls and process objectives is executed. For more information, refer to Importing Risks and Controls into Oracle Internal Controls Manager, page 4-17.

Process Objectives in the Risk Library

The objectives associated with a process are typically viewed in the process details window in the risk library.

| Topic | Navigation Path |
|---|--|
| View Process Objectives associated with a process | Using the Business Process Owner (or equivalent) responsibility, click the Risk Library tab and the Processes subtab. Drilldown into the relevant process and scroll to the Objectives section. |

However, you can also view and set process objectives in the context of related risks. As noted earlier, these are the risks that arise as a result of the objectives orienting the process in a particular direction.

| Topic | Navigation Path |
|---|---|
| View Process Objectives in the context of risks | Using the Business Process Owner (or equivalent) responsibility, click the Risk Library tab and the Risks subtab. Drilldown into the relevant risk and select the Objectives subtab. |

By clicking the Remove/Add buttons, OICM allows you to associate specific process objectives to a particular risk.

Process Attributes

The following table gives further information on select fields in the process details page.

| Field | Description | Seeded Values | Lookup Type | Accessibility Level |
|---------------------|---|---|---|---------------------|
| Process Owner | The name of the person responsible for the execution of the process | N/A | N/A | N/A |
| Finance Owner | The name of the person responsible for the financial aspects/results of the process | N/A | N/A | N/A |
| Approval Status | Process Approval Status. To be available for use in Oracle Internal Controls Manager, a process must have a status of "Approved" | Approved Draft Pending Approval Rejected | AMW_ PROCESS_ APPROVAL_ STATUS | System |
| Standard Process | Whether the process is considered to be standard or non standard. Non standard processes may possess unique risks and require distinct controls and audit procedures. | Yes No | AMW_ STANDARD_ PROCESS | System |
| Process Category | Process classification. Non-routine processes require more audit focus than Routine processes. An Estimate process is performed for arriving at a financial estimate. | Estimate Non- Routine Routine | AMW_ PROCESS_ CATEGORY | Extensible |
| Significant Process | An indicator of the priority of the process | Yes No | AMW_SIGN IFICANT_ PROCESS | User |

| Field | Description | Seeded Values | Lookup Type | Accessibility Level |
|------------------------|--|---|-------------|---------------------|
| Process Type | <p>You can fine tune the process definition through its Type.</p> <p>"Task" is a unit of work undertaken within a process.</p> <p>"Control Activities" are a unit of work undertaken for the primary purpose of mitigating the risk associated with the process. They can be thought of as controls in the form of processes associated with the process being setup.</p> <p>Process and tasks that are flagged with the appropriate Audit Mode in Oracle Tutor are automatically created in OICM as Control Activities.</p> | <p>Process</p> <p>Sub process</p> <p>Task</p> <p>Control Activity</p> | N/A | N/A |
| Process Classification | Classification for Extensible Attributes. | N/A | N/A | N/A |

Note: OICM allows you to associate processes with specific organizations in the enterprise. You can update process attributes in a particular organization without affecting those attributes in other orgs. For example, you can have different process owners for the same process in different orgs.

Refer to Revising Processes in Organizations, page 3-16.

Process Significance

As noted in the table above, when Processes are created in the risk library, you can set the attribute of Significance using a "Yes/No" flag. For a significant process, OICM allows you to specify the determinants of this attribute i.e. why this process was determined to be significant.

The profile option AMW: Default for Significant Process during process creation can be set to automatically default this value.

| Topic | Navigation Path |
|----------------------------------|---|
| Significant Process Determinants | Using a superuser or equivalent responsibility, click the Risk Library tab and then the Processes subtab. Drill into the Process Details page and scroll down to the Process Significance section. |

The determinants are from a Lookup Type and are user extensible.

Process Owner:

OICM uses the Process Owner field in the following two ways:

1. If you implement "Roles and Privileges" within the application, this field is used to allow access to an organization.

Note: For more information, refer to Roles and Privileges, page 15-1 in OICM.
2. When a process certification is created, OICM uses the process owner field to assign certification tasks. Only process owners can view and certify their processes within a certification.

For example, assume a process certification that involves the process "P2P." If a user "U" is the process owner of this process in the org "US," then U is responsible for certifying P2P in the US org and will receive a notification to that effect. If a process certification is required and the owner of a process is not identified, then notifications to certify the process cannot be sent.

Note: For more information, refer to Process and Organization Certification, page 10-1.

Associating Documents with Processes

Process documentation often becomes the basis for compliance checking performed by auditors. With OICM you can attach any document to a process. The attached document can serve a variety of purposes. For example, it may be descriptive or as a basis for teaching users how to deploy the process.

Tutor Attachments

Oracle Tutor is Oracle's preferred documentation tool. Tutor offers process / procedure authoring, automatic flowcharting, and role based publishing along with predefined business models and flows. Out of the box processes and procedures can therefore be easily modified to represent your business processes in the Oracle E-Business suite. Oracle Tutor is also integrated with Oracle iLearning which allows your managers to verify that their employees have studied the procedures required to perform the job.

Once procedures are developed using Oracle Tutor, you can associate the procedures with applicable processes as well as access them from the process details window in OICM.

To associate documents (from Tutor) with processes

From the Processes window of the Risk Library, click Convert Tutor Document (since Tutor is Oracle's preferred documentation and authoring tool) and then click Attach to attach your documents to a process.

The steps to associate a document with a process are the same as listed in the section Attaching a File to a Process.

Note: Distinguish these files from Tutor Process Authoring files. Unlike the latter, these documents are attached to processes for descriptive / explanatory purposes only.

It is also important to remember that attachments are added to a process (or risk, control, audit procedure object) in the risk library and organization independently. Attachments made in the library are viewable in the library only while those made to a risk library object in a particular organization are not carried over from the org to the risk library automatically.

Other Attachments

Note: The following discussion hold for attaching documents to all risk library and organizational objects (not just processes).

Using the "Attachments" subtab, OICM allows you to attach documentation of virtually any data type to objects in the application like processes, risks/controls, and audit engagements. Attachments result in the revision of the object. In addition to the storage of data in "Oracle Files", the attachment feature supports third party repositories as well. The documents/files can hence be stored in an external document management system and linked to the engagement object.

Prerequisites

The followings two tasks must be completed before you can link any attachments to objects in the application:

1. Set the Self Service Oracle Files Enabled profile option to "Yes" (at the Application level).
2. Set the appropriate documentation repository parameters as follows:

| Topic | Navigation Path |
|--|--|
| Set up parameters for the Application Documentation Repository | Using the System Administrator responsibility, navigate to the Application: Document > Repository. |

Repository Setup

| Select Object: (Test Connection) (Remove) (Add New) | | | | | | | |
|---|----------------------------|----------------------------|-------------------|--------------------------------|--------------------------------|----------|------------------|
| Short Select Name | Name | Description | Product Type | Service URL | WebDav Connection URL | Sequence | Certificate Path |
| <input type="radio"/> TNS | Oracle Business Suite | Oracle Business Suite | | | | | |
| <input type="radio"/> OFNA | Oracle Files North America | Oracle Files North America | Oracle Files V1A2 | http://documents.oracleids.com | http://documents.oracleids.com | | |

For the appropriate instance, set the required parameters as follows:

| Parameter Name | Description |
|-----------------------|--|
| Service URL | Used to check whether the Oracle Files Online (OFO) instance is up and running. For testing purposes only. |
| WebDAV Connection URL | URL that is used to open a DEV (http) connection with OFO. |
| Sequence | An ordering sequence number. |

At any time during the execution of the audit, you can now link attachments to the Audit Engagements or other objects in the application.

| Topic | Navigation Path |
|--|---|
| Attach a file to a risk library or organizational object | In the details page of the object or the Audit Engagement, navigate to the Attachments subtab |

Home Audit Operations **Organizational Objects** Organizations Risk Library Setup

Engagements Assessments Findings Remediation

Audit Operations Engagements >

Audit Engagement: Americas Sales Audit Q1 2006

Report: Generate

Team: Internal Audit Type

Sign Off Status: Not Submitted Description

Name: Americas Sales Audit Q1 2006
 Number: 1A10024
 Manager: Sherman, Anita
 Status: Active
 Start Date: 12-Feb-2006

View:

Objectives Scope Tables Controls Risks Processes Organizations Findings **Attachments** Settings People

Attach Documents

Attached Documents

Add Attachment:

| Name | Modified By | Last Modified Date | Repository | Details | Detach |
|----------------|-------------|--------------------|------------|---------|--------|
| No data exists | | | | | |

Upload Desktop File To EES Repository
 Upload Desktop File From Office

Attached folders

Add:

| Name | Description | Attachment Category | Last Modified By | Last Modified Date | Default Folder | Repository Details Detach |
|----------------|-------------|---------------------|------------------|--------------------|----------------|---------------------------|
| No data exists | | | | | | |

Linking Key Accounts with Processes

To certify a financial statement, the impact of the different business processes that affect the financial items on the statement first needs to be understood. Each financial item is an account or consolidation of accounts and an integral part of the processes that affect it. It is imperative that the processes behind financial items be recognized and incorporated into the financial audit.

OICM therefore enables the mapping of processes to natural accounts defined in the system. These accounts are based on the natural account segment definition in the chart of accounts.

Note: For more information on natural accounts and their definition, see the *Oracle Applications Flexfields Guide*.

There are two ways to link accounts with processes in OICM.

- Manually link key accounts with processes
- Import the process and key account associations

Pre-Requisites to linking Accounts and Processes

Both the above methods require the following pre-requisites:

1. Import the Financial Accounts

The OICM application enables you to import your financial statement structure, chart of accounts and the relationship between financial items and key accounts from your financial reporting application, whether it is Oracle Financial Statement Generator (FSG) or any another application.

By setting the profile option AMW: Use Oracle Financial Statement Generator, you define the source of the financial accounts and statements that will be recognized by the application.

- **Financial accounts and statements originate in FSG reports**

Financial Statement Generator (FSG) is a powerful ad hoc reporting tool and is a component of the Oracle General Ledger module. Using the FSG, you can build report "row" and "column" objects and merge them into financial reports. The row objects are typically the relevant financial items of the report. Once FSG reports are built, they can be saved in the system for reuse.

By default this profile option is set to "Yes" and indicates that the financial items from reports created in Oracle General Ledger using FSG are automatically available to OICM.

For financial items based on FSG reports, you also need to set the **AMW: Natural Account Value Set** profile option. This option defines which financial accounts will be recognized by OICM. The natural account value set identifies the accounts that can be certified i.e. these accounts will be displayed in the financial certification detail windows. Note that the natural account value set is only valid for FSG reports created in the Oracle E-Business Suite. If a third party reporting tool is used, then this profile option is ignored.

- **Financial accounts and statements originate in an external third party system.** The financial statements and items are maintained and stored in the third party system.

If you use an external third party reporting set, then the profile option AMW: Use Financial Statement Generator must be set to "No." In this case you will need to set the profile options shown below to map the financial items in the third party system to OICM. These third party items will then be recognized by OICM.

The following table lists the profile options that must be seeded if Financial Statement Generator Reports are not used.

| Profile Option | Description | Required Columns | Data Type |
|--|---|---------------------------|-----------|
| AMW: View for Financial Item Descriptions in External Apps | Contains the View Name to get the Financial Items Language Specific Name. | FINANCIAL_STATEMENT_ID | Number |
| | | FINANCIAL_ITEM_ID | Number |
| | | NAME | Varchar2 |
| | | LANGUAGE | Varchar2 |
| | | SOURCE_LANGUAGE | Varchar2 |
| AMW: View for Financial Item and Account Relation in External Apps | Contains the View Name to get the Financial Statements to Items to Key Account Mapping. | FINANCIAL_STATEMENT_ID | Number |
| | | FINANCIAL_ITEM_ID | Number |
| | | NATURAL_ACCOUNT_ID | Number |
| | | | |
| AMW: View for Financial Items in External Apps | Contains the View Name to get the Financial Items. | FINANCIAL_STATEMENT_ID | Number |
| | | FINANCIAL_ITEM_ID | Number |
| | | PARENT_FINANCIAL_ITEM_ID | Number |
| | | | |
| AMW: View for Financial Statements in External Apps | Contains the View Name to get the Financial Statements. | FINANCIAL_STATEMENT_ID | Number |
| AMW: View for Financial Statement Descriptions in External Apps | Contains the View Name to get the Financial Statements Language Specific Name. | FINANCIAL_STATEMENT_ID | Number |
| | | NAME | Number |
| | | DESCRIPTION | Varchar2 |
| | | LANGUAGE | Varchar2 |
| | | SOURCE_LANGUAGE | Varchar2 |
| AMW: View for Key Account Names in External Apps | Contains the View Name to get the Key Accounts. | NATURAL_ACCOUNT_ID | Number |
| | | NAME | Varchar2 |
| | | LANGUAGE | Varchar2 |
| | | SOURCE_LANGUAGE | Varchar2 |
| AMW: View for Key Account in External Apps | Contains the View Name to get the Key Accounts. | NATURAL_ACCOUNT_ID | Number |
| | | NATURAL_ACCOUNT_VALUE | Varchar2 |
| | | PARENT_NATURAL_ACCOUNT_ID | Number |
| | | | |

2. Run the Import Natural Accounts Concurrent Program

Run the concurrent program Import Natural Accounts to bring all relevant financial items into the OICM application tables.

Note: For more information on importing financial statements, refer to B. Import the Financial Statements to be Certified., page 11-3

Manually link Significant Accounts with Processes

| Topic | Navigation Path |
|---|--|
| Manually link Significant Accounts with Processes | <p>Using the Business Process Owner (or equivalent) responsibility, click the Risk Library tab and the Processes subtab.</p> <p>For the relevant process, click the Modify icon to access the Process Hierarchy Workbench. Drilldown into the appropriate process and select the Update dropdown.</p> <p>Select the Significant Accounts subtab to add and/or update accounts.</p> |

All natural accounts defined in the associated value set appear in the list of values. You can link multiple Significant Accounts with a process.

Import the process and key account associations

Instead of linking processes with accounts individually, you may import all process key account associations in a single step.

1. In the Risk Library > Import tab select "Import Process to Key Account Associations."
2. Select viewer settings (Excel 1997/2000) and then update the displayed spreadsheet with the appropriate data.
3. Select "Oracle - Upload" from the spreadsheet menu bar.

Note the following points with regard to the import of Process-Key Account Associations using Oracle Web ADI.

- The Financial Statement and Financial Item fields can be used to filter the values in the Key Account column.
- Web ADI uploads the data from the spreadsheet into the AMW_KEY_ACC_INTERFACE table. A concurrent program then uploads the data from the interface table to the base tables. You may choose to submit this program automatically during the upload. Any errors that occur during the import process are flagged as errors with appropriate error messages.
- Once data is imported, the profile option "AMW: Process to Key Account Associations - Delete after import?" provides users with the option of deleting the rows from the interface. The default value is set to "Yes" so that once the rows are successfully imported, they are automatically deleted from the interface.

The following table lists the fields in the import spreadsheet:

| Field Name | Mandatory | Validation |
|---------------------|-----------|---|
| Process Name | Yes | All valid processes in the system |
| Financial Statement | No | All valid financial statements in the system. These statements originate in Oracle FSG or 3rd party reports. |
| Financial Item | No | All valid financial items in the selected statements. If the statements are Oracle FSG reports, then these items are typically "row" objects. |
| Key Account | Yes | All valid accounts belonging to the selected financial statement and item. If the financial statement and item filters are left blank, then the LOV shows all accounts. |

Organizations in Oracle Internal Controls Manager

Note: For detailed information on seeding risk library objects (other than processes) into the risk library, refer to Risks and Controls in Oracle Internal Controls Manager, page 4-1 and Audit Procedures in Oracle Internal Controls Manager, page 5-1.

Once the risk library is seeded, most remaining setups in the application are done within the context of a particular "Organization." It is advantageous for companies to standardize their business processes across these organizations. Benefits include common process methodologies, economies of scale and learning, etc.

In a dynamic environment however, processes are subject to change that can be unique to an organization. In addition, for enterprises that span multiple locations, there can be a variety of environments in which the processes are executed. These dissimilar settings often result in a need to modify processes in particular organizations. Oracle Internal Controls Manager therefore provides the ability to create the following:

- Process Variations (in the risk library). The variation can be later associated with an organization.
- Process Exceptions (in individual organizations).

Note: For more details on process variations, refer to Revising Processes in the Risk Library - Part 2 (Process Variation Management), page 3-12. For more details on process exceptions, refer to Process Revisions in Organizations, page 3-16.

To Setup Organizations in Oracle Internal Controls Manager

Organizations in Oracle Internal Controls Manager must be "Auditable Units." An Auditable Unit is any logical division or grouping of the enterprise that is available as an organization classification in the Oracle E-Business Suite. For example, a legal

entity, operating unit, company cost center, inventory organization, or any other organization can be classified as an Auditable Unit.

Prerequisite

Before you can set up an organization as an Auditable Unit, you need to first seed the following profile options.

- AMW: Subsidiary Value Set for Auditable Units Required. This value set should be the same as the one used by the "Company" segment in your chart of accounts.
- AMW: Line of Business Value Set Optional. This can be any value set that is used for line of business values.

Note: If you have Oracle Daily Business Intelligence installed, this value set corresponds to Line of Business value set that is used in the Management flexfield.

Setting up Auditable Units in Oracle Human Resources

The following is a summary of the steps that must be performed in Oracle Human Resources.

Note: For detailed information on setting up organizations, refer to *Using Oracle HRMS – The Fundamentals*.

1. In Oracle Human Resources, navigate to the Work Structures > Organizations > Description form.
2. Enter the primary attributes of the organization like the Name, Dates it is valid, and Location.

Organization Classification

3. In the Organization Classification section, select Auditable Unit. Click the Enabled check box and then Others to drill into the details of the Auditable Unit.
4. Select the Subsidiary value set for this Auditable Unit. The list of values defaults the value set from the AMW: Subsidiary Value Set for Auditable Units profile option. Next, select a subsidiary value. The Auditable Unit is now associated with this Subsidiary.

It is important to note that the Auditable Unit goes beyond the concept of a subsidiary. In the Organization window, your organization (that is now an Auditable Unit) can also be set up with any other classification like an "Inventory Organization" or a "Legal Entity."

As an example, if you are investigating the internal controls of inventory organizations in your enterprise, then each of these inventory organizations must also be tagged as an Auditable Unit and associated with a subsidiary. You can have several organizations like Inventory Organizations under the same subsidiary. Each of these Auditable Units will also be linked to this subsidiary.

On the other hand, assume your domain of interest is a Legal Entity that spans multiple subsidiaries. In this case you need to set up multiple Auditable Units, with one Auditable Unit for each subsidiary. Each of these Auditable Units will also be tagged as a Legal Entity.

5. Select the Line of Business value set for this Auditable Unit. This step is optional. The list of values defaults the value set from the AMW: Line of Business Value Set profile option. Select a Line of Business value that will be associated with the Auditable Unit.

Note that multiple Audit Units can be associated with a particular Line of Business value.

Associate Page Search

When you associate a process to an organization, you can optionally look for the organization in the Associate search window using the following dimensions:

- Organization Name.
- Organization Location.
- Subsidiary. Subsidiaries in Oracle Internal Controls Manager map to "companies." The list of values for this field shows the values of the Accounting Flexfield Company segment. Once you select a subsidiary in the Search window, the resulting page shows all the organizations linked to this subsidiary.
- Line of business. The list of values for this field shows the values from the Line of Business value set that have been associated with existing Auditable Units. Once you select a Line of Business in the Search window, the resulting page shows all organizations linked to this Line of Business value.

Linking Processes with Organizations

Processes are originally imported into the Risk Library in Oracle Internal Controls Manager. Risks, controls, and audit procedures must be associated with each other and with processes before an audit opinion can be issued. These associations are initially performed in the Risk Library.

As different organizations may perform different processes, Oracle Internal Controls Manager allows you to associate processes with specific organizations in the enterprise i.e. processes are mapped to the organization structure of the enterprise. All links with risk library objects associated with the process are carried over into the associated organizations. You can view them from the organization views in the application.

| Topic | Navigation Path |
|--------------------------------------|--|
| Linking Processes with Organizations | Using an appropriate responsibility, navigate to the Risk Library tab and the Processes subtab to access the "Associate to Organization" and "Synchronize to Organizations" buttons. |

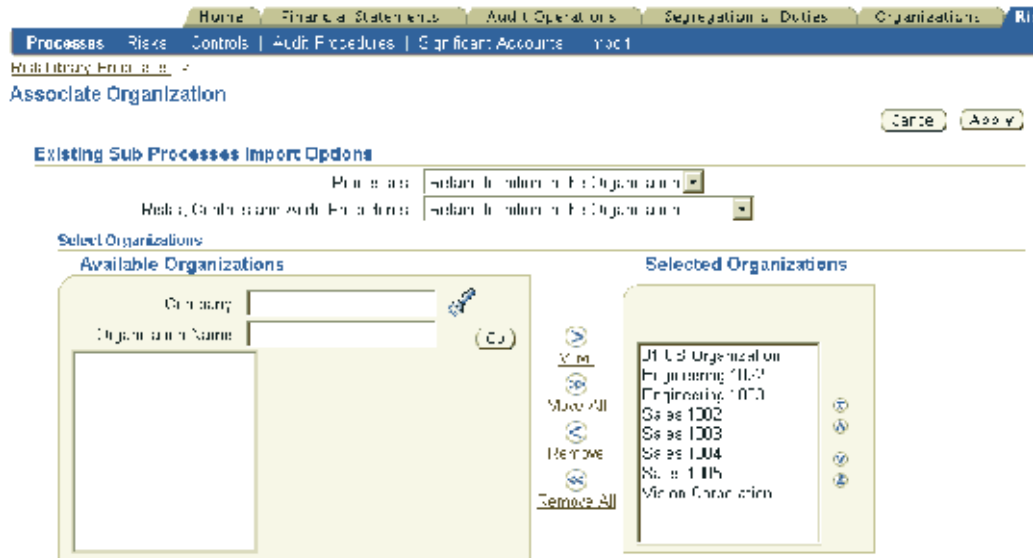
The view of processes in this window is the Approved Hierarchy i.e. only approved processes can be associated with organizations. Remember that a process cannot appear in this view until and unless the following conditions are met:

- The process is approved.
- The process has an approved path to "All Processes" i.e. the top level process node in the hierarchy i.e. if any processes exist above it in the hierarchy, those processes must also be approved.

When you link or re-associate processes from the risk library to an organization with an existing hierarchy of processes, the existing hierarchy (if any) is not automatically overridden. Instead, the application provides you with the several options.

These options are discussed below.

Associate to Organizations



By default, all organizations are listed in the trailing window "Selected Organizations," that are not currently associated to the process (you cannot associate the same process to an organization twice, use the Synchronize to Organization" button instead). By clicking apply at this point, all the organizations in the trailing window are automatically associated. To search for a subset, you can move these back to the "Available Organizations" leading window and filter them by company and organization name.

While associating the process to the organization, the application provides you with the following options with respect to its subprocesses:

1. Retain definition in the Organization.

In this case, the attributes of the sub processes and their downward hierarchy are not overridden.

For example, assume that process P1 in the risk library is being associated with Org O1. Process P1 has a subprocess P2 which in turn has no subprocesses. If P2 exists in O1 with a child P3, then associating P1 to O1 (with the option to "Retain definition in the Organization), results in the structure

```
P1
|
P2
|
P3
```

2. Synchronize with the library definition

In this case, the attributes of the sub processes and their downward hierarchy are overridden by the current library definition. In the case of the above example, the resulting structure in O1 is

```
P1
|
P2
```

Synchronize with Organizations

Discrepancies between a process in a particular organization and its original form in the risk library can originate in the following ways:

1. You may subsequently add or change a risk, control, procedure, account associated with the process in the risk library. You can also change the process structure itself i.e. add/delete children in the risk library. These additions and changes are not automatically migrated to the processes that have been mapped to organizations in the application.
2. You can also create a process exception i.e. modify the process in a particular organization. These changes are not reflected in the process structure within the risk library.

You can choose to synchronize the process and/or its subprocesses, the process hierarchy and/or its attributes, associated risks, controls, and audit procedures, as well as people with designated roles and privileges on the process. Based on the synchronization options followed, specific changes made in the context of an organization will be obliterated.

The screenshot shows the 'Synchronize Process: Accounting to Financial Reports' dialog box. The 'Synchronization Options' section includes the following settings:

- Processes:** Selected Process and Sub Processes
- ☐ Synchronize Process Hierarchy
- ☐ Synchronize Process Attributes
- Risks, Controls and Audit Procedures:** Retain definition in the Organization
- Process People:** Retain definition in the Organization

The 'Select Organizations' section shows two lists: 'Available Organizations' and 'Selected Organizations'. The 'Available Organizations' list is empty, and the 'Selected Organizations' list is empty. The 'Move' button is highlighted.

Note: Only processes that have been approved in the Risk Library can be associated with the organization. However, once linked to an organization, the process must also be approved in the organization.

Process (and other Risk Library) Attachments

Note that attachments are added to a process (or risk, control, audit procedure object) in the risk library and organization independently. Drill down into the process and then select the "Attachments" link.

Attachments made in the library are viewable in the library only while those made to a risk library object in a particular organization are not carried over from the organization to the risk library.

Linking Risks and Controls with Organizations

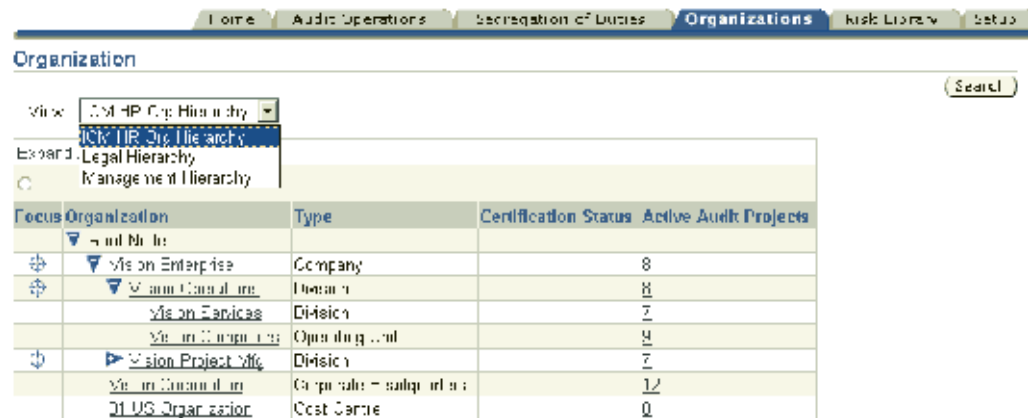
You can similarly link risks and controls directly with organizations.

| Topic | Navigation Path |
|--|---|
| Linking Risks and Controls directly with Organizations | Using a Super User (or equivalent) responsibility, navigate to the Organizations tab and drill into the appropriate organization to access the Risks and Controls subtab. |

Viewing Organizations

Three hierarchy views are available for organizations:

1. Custom Hierarchy. This is the hierarchy of organizations as defined in the Oracle HR module and entered in the "AMW: Org Security Hierarchy" profile option.
2. Legal Hierarchy. This is the hierarchy of subsidiaries (companies) in the Subsidiary Value Set. The value set name must be entered in the "AMW: Subsidiary Value Set for Audit Units" profile option.
3. Management Hierarchy. This is the hierarchy of LOB's in the LOB Value Set. The value set name must be entered in the "AMW: LOB Value set for Audit Units" profile option.



| Focus | Organization | Type | Certification Status | Active Audit Projects |
|-------|--------------------|----------------------|----------------------|-----------------------|
| | Vision Enterprise | Company | 8 | |
| | Vision Corporation | Division | 8 | |
| | Vision Services | Division | 2 | |
| | Vision Project Mfg | Operating Unit | 4 | |
| | Vision Corporation | Company - subsidiary | 12 | |
| | Vision Corporation | Cost Center | 0 | |

Type here is the HR defined organization type.

Process Approvals & Change Management

This chapter covers the following topics:

- Process Approvals in Oracle Internal Controls Manager
- Process Revisions in Oracle Internal Controls Manager
- Process Deletions (Removals and Disassociations)
- Submitting Processes and Process Revisions for Approval
- Process History

Process Approvals in Oracle Internal Controls Manager

The creating and importing of processes in OICM is discussed in the previous chapter. These processes are created in "Draft" status and must go through an approval mechanism as follows:

A process is created with a status of "Draft." When submitted for approval, the process status becomes "Pending Approval." Note that while in a Pending Approval state, the attributes or list of children of the process cannot be changed. If approved, its status becomes "Approved" and the process can then be used in the application.

Note: The exception to the general case described above is that you can import a process as approved using WebADI provided:

- The Process Approval Status entered in WebADI is "Approved."
- The OICM process parameter "Approval Required" (described later in this section) is set to "No."

Process Verification

The verification of business processes in an organization is a major portion of the internal audit function. These processes (both manual and automated) are subject to change due to a variety of reasons such as a rapidly changing environment, legislation, changes in other processes, etc. Since the changes can adversely impact process risk exposure as well as the internal controls set up on the process, process changes must be subject to a review and approval mechanism.

Further, the internal audit department must assess the process change to ascertain whether it introduces additional control risks. Risks to internal controls can be captured through a review of the changes to key risks, controls, and business settings. It is hence critical to be able to view version information and historical data for business processes.

Oracle Internal Controls Manager provides a rich functionality in this domain and uses an intuitive workbench to provide features and benefits like the following:

- All processes and process revisions are created in a "Draft" status and must be approved before the process or it's revision can be used in the system. Change notifications are sent to all concerned personnel (ex. process owners) and recipients of these notifications can review the modified processes prior to giving their approval.
- The application maintains a detailed revision history for all processes (including non standard processes) in the entity. Auditors therefore have the ability to view a complete audit trail of changes taking place in the organization and the risk library.
- Before approving a process change, you can compare the revised process with it's prior version to determine whether the change is acceptable. This comparison is crucial in determining the impact of changes/deviations on associated processes. Through a hierarchy viewer, you can also see which associated business processes are impacted by the change.

Note: This method for verification of processes does not apply to the approval of Risk, Control and Audit Procedure objects. Those objects use Oracle Approvals Management for revision control.

Refer to Risk Library Change Control, page 6-1 as well as the *Oracle Approvals Management Implementation Guide*.

Process Approval Setup - Process Parameters

There are different submission and approval "environments" predicated in OICM based on the value of the application's "Process Parameters." These parameters determine how process approvals function in the Risk Library and in organizations and provide flexibility in the creation and modification of processes.

| Topic | Navigation Path |
|---|--|
| Set up Process Parameters for Process Approvals in both the Risk Library and OICM Organizations | Using the Business Process Owner (or equivalent) responsibility, click the Setup tab and then the Risk Library subtab Navigate to the Process Parameters Window to update Risk Library and Organization Parameters. |

The screenshot displays the Oracle Internal Controls Manager interface. At the top, a navigation bar shows tabs for 'Home', 'Business Processes', 'Segregation of Duties', 'Organizations', 'Risk Library', and 'Setup'. The 'Setup' tab is active. Below the navigation bar, there are two main sections: 'Risk Library Parameters' and 'Organization Parameters'. The 'Risk Library Parameters' section includes fields for 'Approval Color', 'Approval Independent of Descendant's Approval Status', and 'Process Code Prefix'. The 'Organization Parameters' section includes a search bar and a table with columns for 'Organization Name', 'Approval Option', and 'Approval Required'.

Update Risk Library Parameters

Home > Business Processes > Segregation of Duties > Organizations > Risk Library > Setup

Issue Management > Configure > Risk Library > Approvals > Value Sets

Update Risk Library Parameters

Approval Option: Approval Independent of Descendants Approval Status

Approval Required: No

Process Code Prefix: ICM_

Cancel Submit

The following parameters must be set up before you can use the process approval mechanism in OICM.

Approval Option

1. Approval Independent of Descendants Approval Status

This option enables the independent approval of a process irrespective of the status of others processes below it in the hierarchy. You can hence submit and approve the process even if its subprocesses are not approved.

2. Automatically Approve all Descendants

On approval of a process, all its descendants are also approved i.e. all sub processes at any level (children, grandchildren etc.) are also approved.

3. All Descendants should be Approved

When this option is active, a process can be submitted for approval only if all its descendants are already approved.

The Approval Option setting can effectively limit the choice of actions that can be performed on lower level processes in a hierarchy when a higher level process is submitted for approval. For example, if the "Automatically Approve all Descendants" option value is active, no changes are allowed in the downward hierarchy of a submitted process till that process is approved.

Note: Changes in the Approval Option setting are allowed only if no submitted processes are awaiting approval in the system i.e. there are no processes with a status "Pending Approval." In this case there are no processes that are currently locked in the system.

Approval Required

This parameter determines whether Oracle Workflow will be used in process submission or whether the process is automatically approved.

If Approval Required is set to "No" and the Approval Option is "Approval Independent of Descendants Approval Status," then process approvals take place immediately. If Approval Required is set to "Yes," then a workflow approval routing is initiated when the process is submitted for approval.

Note: For more information on the use of Workflow for approvals in OICM, see the next section Submitting Processes and Process Revisions for Approval.

Process Code Prefix

Enter a code that is used as a prefix in process code nomenclature. This setup is valid in the Risk Library only but carries over with processes in the organizational context.

Update Organization Parameters

Update Organization Parameters

⚠ TIP Parameters are disabled for Organizations where some processes are in Pending Approval Status

Search

Organization Name:

☐ Exclude organizations that have not been configured

| Organization Name | Approval Option | Approval Required |
|-------------------|---|-------------------|
| Engineering 002 | Approval Independent of Descendants Approval Status | No |
| Engineering 003 | Approval Independent of Descendants Approval Status | No |

Cancel Submit

When an organization is registered with OICM, these values default from the OICM Risk Library.

You can maintain the settings (as described in the previous section) for a particular organization in this window. For example, if the Approval Required parameter is "Yes" in the Risk Library, the same parameter can have a value "No" in Organization "B." Process approval is then required in the RL but not in org "B."

Process Hierarchies

Processes can be viewed in two hierarchies in OICM - the "Approved Hierarchy" of processes and the "Latest Hierarchy" of processes. The application distinguishes between these two hierarchies as follows:

Approved Hierarchy

The primary view of processes in the Risk Library or in an organization is the Approved Hierarchy.

| Topic | Navigation Path |
|---|---|
| Accessing the Approved Hierarchy of Processes | <p>Using the OICM Super User (or equivalent) responsibility, click the Risk Library tab and then the Processes subtab.</p> <p>Alternately, navigate to the Organizations tab and then drill into a particular organization to view the Approved Hierarchy in that organization.</p> |

| | | | | | | | | | |
|---|------|-----------------------|---------|----------|------------|---------------|--------------------|-------------|----------|
| Home Project Information Add Operators Setup Organization Organization Risk Library Setup | | | | | | | | | |
| Processes Risks Controls Audit Procedures Significant Accounts Inputs | | | | | | | | | |
| Processes (Screen) | | | | | | | | | |
| Select Process: Select Organization Expand All Collapse All | | | | | | | | | |
| Select | name | Processes | Revised | Revision | Risk Count | Control Count | Organization Count | Significant | Standard |
| | | Processes | | | | | | | |
| | | Work Management | | 4 | 5 | 7 | | Yes | Yes |
| | | CRM | | 13 | 14 | 11 | 13 | Yes | Yes |
| | | Customer Relationship | | 7 | 6 | 6 | 11 | Yes | Yes |
| | | Product Line | | 7 | - | 2 | 12 | Yes | Yes |

A process cannot appear in this view until and unless both the following conditions are met:

- The process is approved.
- The process has an approved path to "All Processes" i.e. the top level process node in the hierarchy i.e. if any processes exist above the process in question in the hierarchy, those processes must also be approved.

Note: The top level process "All Processes" behaves differently from all the other processes. It is always considered to have a status of "approved," a revision number of 1, and is frequently denoted as just "ALL."

Note that there is no status column in this view as all processes are approved. If approved processes do not exist in the system, the Approved Hierarchy is simply the All Processes node.

Latest Hierarchy (and the Process Hierarchy Workbench)

| Topic | Navigation Path |
|---|---|
| Accessing the Latest Hierarchy of Processes | <p>Using the OICM Super User (or equivalent) responsibility, click the Risk Library tab and then the Processes subtab. Alternately, navigate to the Organizations tab and then drill into a particular organization to view the Approved Hierarchy in that organization.</p> <p>In the Approved Hierarchy view, click on the Modify Process icon for the appropriate process to access the "Process Hierarchy Workbench."</p> |

The resulting view is the current hierarchy under that process and is referred to as the "Latest Hierarchy."

|----P4(A,1,X)

Process P3, though itself an approved process, does not have an approved path to the root node "All Processes" since P2 is in Draft status. Hence P3 does not appear in the Approved Hierarchy.

Note: The above scenario assumes the user has access to all processes in the firm. For more information, refer to Process Hierarchy Views in OICM, page 3-7 as well as Roles and Privileges in OICM, page 15-1.

In the case of revised processes, the current (latest) approved revision is displayed in both Approved and Latest Hierarchies with status "Approved" and unapproved revisions are displayed in the Latest Hierarchy only with status "Draft."

It is important to remember that only approved processes (processes that appear in the Approved Hierarchy) can be assigned to organizations and used in the application.

Process Hierarchy Views

The previous examples detailed the "Approved" and "Latest" hierarchy under the "All Processes" node.

However, the typical user in OICM only gets to view those processes that list them as the owner (under the My Processes tab). In this case, users that cannot access the "ALL Processes" node (those who are not Superusers) will access a top level dummy process node called "My Processes." The user's processes are listed under this node in hierarchical form.

Example 1

As an example, assume the **Latest Hierarchy** is the following:

ALL

|

|----X(D,1,X)

|

|----P(A,2,X)

|

|----Q(D,1,X)

When the owner of P views the **Approved Hierarchy**, the view is simply:

My Processes

and nothing more.

This is because Process X is not approved and so P does not have an approved path to "All Processes" node. Therefore P is not yet been added to the approved hierarchy of ALL.

However, when the owner of P views the **Latest Hierarchy**, the view is:

My Processes

|

|---P(A,2,X)

```
|
|---Q(D,1,X)
```

Now assume that Process X gets approved. The view in the **Approved Hierarchy** for the owner of P is:

My Processes

```
|
|---P(A,2,X)
```

The view in the **Latest Hierarchy** (again for the owner of P) is now:

My Processes

```
|
|---P(A,2,X)
|
|---Q(D,1,X)
```

Example 2

Assume the latest hierarchy is:

ALL

```
|
|-----X(D,1,X)
| |
|---Q (A,1,X) |---P(A,2,X)
|
|---Q(A,1,X)
```

The owner of P views the **Approved Hierarchy** as:

My Processes

```
|
|---Q(A,1,X)
```

This is because the owner of P also owns Q in that specific hierarchy. However P is not yet present in the Approved Hierarchy as X is not approved.

The owner of P views the **Latest Hierarchy** as:

My Processes

```
|
|---P(A,2,X)
|
|---Q(A,1,X)
```

Note that Q is only visible in relation to P.

Process Approval Examples

The following examples provide an overview of process approval functionality in OICM. The process approval mechanism is largely dictated by the value of the Approval Option parameter.

In the following examples, unless otherwise stated, assume that the Approval Option parameter is set to "Approval Independent of Descendents Approval Status." P(A/D,1,X) denotes a Process P that has a status A-Approved or D-Draft, a revision number 1, and attribute X[n].

Approval Options are denoted by A1, A2, A3.

A1 - all processes are approved independently.

A2 - everything below the approved process is automatically approved.

A3 - allows submission for approval only if all processes below the process in concern are already approved.

Example 1

Suppose the **Latest hierarchy** is the following:

ALL

|

| -- P1 (D,2,X)

| |

| | --- P4(A,1,X)

|

| -- P2(D,1,X)

|

| -- P3(A,1,X)

In this case the **Approved Hierarchy** is simply

ALL

Assume that P1 is now approved. Then P4 has an "approved" path to the root and hence both P1 and P4 are added to the Approved Hierarchy.

Approved Hierarchy is now

ALL

|

| -- P1 (A,2,X)

| |

| | --- P4(A,1,X)

Note that though P3 is an approved process, it does not yet have an approved path to the root and so does not appear. The above scenario hold true for any value of the Approval Option parameter.

Example 2

In this example, assume the Approval Option parameter is A2.

The **Latest Hierarchy** is as follows:

ALL

```
|
|-- P1 (D,2,X)
| |
| | --- P2(D,1,X)
| |
| | ---P3(D,1,X)
| |
| | ---P4(A,1,X)
|
|--P2(D,1,X)
|
|--P3(A,1,X)
```

Suppose P1 is submitted for approval and then later approved. Since the active Approval Option parameter is A2, all the descendants of P1 are also immediately approved. This means that P2 and P3 are also approved.

The **Latest and Approved Hierarchies** are now as shown below:

ALL

```
|
|-- P1 (A,2,X)
| |
| | --- P2(A,1,X)
| |
| | ---P3(A,1,X)
| |
| | ---P3(A,1,X)
|
|--P2(A,1,X)
|
|--P3(A,1,X)
```

If the Approval Option parameter had a value of A3, then the process P1 could not even be submitted for approval due to the presence of a non approved descendant.

Process Rejection

When a process is rejected, its status is set back to "Draft." If the rejection takes place in an environment where the Approval Option is "Automatically Approve all Descendents," then all locks in the downward hierarchy of the process are released.

As and when required, changes can be made again to the process and the process then resubmitted for approval.

Process Revisions in Oracle Internal Controls Manager

A process is considered to be revised when:

- Any of its attributes are changed. Note that a change in a process attachment also results in a process revision.
- Its list of children changes. These are child processes immediately below the process being investigated. Changes in processes at any other level do not result in a revision.
- Its list of associated risks changes.
- Its list of associated controls changes.

Once revised, a new process revision is created with status Draft and must be submitted for approval. All revisions must go through the same approval mechanism described in the previous section. The revision can then be approved or rejected. If rejected, the process remains in status Draft and the previously approved version remains as the current approved process.

Approved processes (including approved process variations and exceptions) can be revised in both the risk library and individual organizations.

Revising Processes in the Risk Library - Part 1

Revising approved processes is done in the Process Hierarchy Workbench of the Risk Library.

Note: Reordering processes and subprocesses ("Order Children" button in the Process Hierarchy Workbench) does not constitute a process revision and hence needs no approval.

| Topic | Navigation Path |
|---|---|
| Accessing the Latest Hierarchy of Processes | Using the OICM Super User (or equivalent) responsibility, click the Risk Library tab and then the Processes subtab. In the Approved Hierarchy view, click on the Modify Process icon for the appropriate process to access the "Process Hierarchy Workbench " and then drill into the appropriate process. |

Home | Audit Operations | Segregation of Duties | Organizations | **Risk Library** | Setup

Processes | Risks | Controls | Audit Procedures | Significant Accounts | Import

Risk Library: Processes > Process Hierarchy/Workbench >

Process Details: Receive Invoice

Initial to Page | Update | Go

Process Code: RV Group: SOX
Revision Number: 4000 Approval Status: Approved
Is Parent Process: No Standard Process: Yes
Description: Receive Invoices

Basic Information | **Significant Accounts** | Risks | Controls | Audit Procedures | Organizations | Attachments | Page

Process Type: Process Standard Process Name:
Process Category: Estimate Control Activity Type:

Process Flow Chart

▼ Process Significance

Process Significance Determinants

| Element |
|--|
| Contributes to achievement of major goals and objectives of the business |
| Contributes to achievement of financial control assertions |
| Material financial statement materiality is not Significant |

You may update any and all facets of draft or previously approved processes. You can also update risk library objects associated with the process. Select the Update drop down menu choice and then navigate to the appropriate subtab like Accounts, Risks, Controls, etc. to make any changes.

Home | Audit Operations | Segregation of Duties | Organizations | **Risk Library** | Setup

Processes | Risks | Controls | Audit Procedures | Significant Accounts | Import

Risk Library: Processes > Process Hierarchy/Workbench > **Process Details: Receive Invoice** >

Update Process Attributes: Receive Invoice

Cancel | Apply

Process Code: RV
Display Name: Receive Invoice
Description: Receive Invoices

Basic Information | **Process Significance** | Objectives | Significant Accounts | **Risks/Controls** | Variation | Attachments

Select Risk and ... (down arrow) | (Add Risk)

Select All | Select None

| Select | Name | Likelihood | Impact | Approval Status | Description | Material | Material Value | Update Controls |
|--------------------------|---|------------|--------------|-----------------|---|----------|----------------|-----------------|
| <input type="checkbox"/> | Bad Credit | Unlikely | Major | Draft | | No | | + |
| <input type="checkbox"/> | Bad Timing | Most Times | Catastrophic | Approved | Delivering | Yes | | + |
| <input type="checkbox"/> | Customer Default on Accounts Receivable | Often | Major | Approved | Customer Default on Accounts Receivable | Yes | | + |

The LOV's for adding Risk Library Objects display both Draft and Approved objects. However, you cannot submit a process for approval until and unless all associated objects have an Approved status.

Once the modification is complete, you are ready to approve/submit the process.

Revising Processes in the Risk Library - Part 2 (Process Variation Management)

A primary task in setting up OICM is to create processes that accurately reflect the business flows of the enterprise. These processes must then be mapped to the firm's organizational structure. Risks, controls and audit procedures are created and executed in the domain of business processes.

Note: For detailed information on setting up processes in OICM, refer to Overview of Process Setups in Oracle Internal Controls Manager, page 2-1.

For more informations on the organizational structure that is supported in the application, refer to Organizations in Oracle Internal Controls Manager, page 2-29.

It is advantageous for companies to standardize their business processes across organizations and geographic regions. Benefits include common process methodologies, economies of scale and learning, etc.

By virtue of its own unique environment however, an organizational unit within the enterprise may be running a derivative of the standard process. To handle such a process alteration, OICM allows you to create process variations and process exceptions. The application distinguishes between the two as follows:

- Process variations are modifications of standard processes created in the risk controls library of the application. The process alteration is realized in the context of the design of the process. Justification for the variation is made with regard to changes in its design as compared to the standard process. The process variation can be later associated with an organization.
- Process exceptions on the other hand are modifications of both standard and non standard processes in particular organizations. The process alteration as well as justification is realized in the context of a particular organization only. Creating process exceptions is an extremely useful feature when processes and their corresponding risks and controls differ between organizations in an enterprise.

Note: For detailed information on creating process exceptions, refer to Revising Processes in Organizations, page 3-16.

In both cases, the process alteration must be subject to reviews and approvals. The internal audit department must also evaluate the change to ascertain whether it introduces an additional process risk. Additional risk can be mitigated by supplemental or changed controls and audit procedures. Process alterations take the following forms:

- Additional, removed, or replaced processes in a business process hierarchy
- Additional, removed, or replaced risks and controls associated with a process variation / exception
- Changes in the attributes of relevant risk library objects

Setup of Process Variations

The steps to create process variations are listed below:

1. Create the non standard process in the risk library
2. Define the non standard process as the variation of a standard process (optional). You also need to specify reasons/justification for the alteration of the standard process.

As an example, consider a standard procurement process for chemicals and its non standard variation. In the example, the standard materials procurement process has two sub-processes:

- Standard analysis and approvals

- Standard bid

A variation of the above process is used in the case of procurement of hazardous materials. Accordingly the non standard process "NStd Chem Mat Proc" is created as a non standard process. It has three sub processes:

- Non standard analysis and approvals
- Standard bid (the same as the standard sub-process used in the case of a standard materials procurement)
- Inspection

1. Create the non standard process in the risk library

Author or import the non standard process into the application's risk library. Once created in the risk library, a process/process hierarchy can be attached to any organization in the enterprise.

Note: For detailed information on authoring and importing processes in the risk library, refer to Overview of Process Setups in Oracle Internal Controls Manager, page 2-1.

The table below shows the spreadsheet to import the processes given in the above example:

| Process Name | Standard Process | Parent Process Name |
|--------------------|------------------|---------------------|
| Std Chem Mat Proc | Yes | All Processes |
| Std Anal and Appr | Yes | Std Chem Mat Proc |
| Std Bid | Yes | Std Chem Mat Proc |
| NStd Chem Mat Proc | No | All Processes |
| NStd Anal and Appr | No | NStd Chem Mat Proc |
| Std Bid | Yes | NStd Chem Mat Proc |
| Inspection | No | NStd Chem Mat Proc |

The spreadsheet shows a subset of the process attributes tabulated in the process import spreadsheet. To mark a process as non standard, OICM uses a simple Yes/No option.

Note: For more details on all fields in the spreadsheet, refer to the section Process Attributes, page 2-19.

2. Define the non standard process as the variation of a standard process (optional)

| Topic | Navigation Path |
|-----------------------------|---|
| Define a process variations | <p>Using the Business Process Owner (or equivalent) responsibility, click the Risk Library tab and the Processes subtab.</p> <p>For the relevant process, click the Modify icon to access the Process Hierarchy Workbench. Drilldown into the appropriate process and select the Update drop down to access the Variation subtab.</p> |

In the Variation page, this process can be set up as a variation of a standard process. To do this, select "No" for Standard Process and enter the name of the standard process in the Variation region of the page. The non standard process is now a variant of the standard process. It is important to note that only processes that have been set up as standard processes will appear in the LOV for the Standard Process field.

In our example, "NStd Chem Mat Proc" as well as "NStd Anal and Appr" are setup as variations of the standard processes "Std Chem Mat Proc" and "Std Anal and Appr." Finally enter the reasons and justification for the variation.

Comparing standard and variant process

| Topic | Navigation Path |
|---|--|
| Comparing standard and non standard processes | <p>Click the Risk Library tab and then the Processes subtab</p> <p>Drilldown into the non standard process</p> |

In the process details window of the non standard process, click the Variation Exception button to compare the standard process with its variation.

Note that you can have an unlimited number of non standard processes that are variants of a standard process. However, at any given time you can only compare the current non standard process with the standard process it is associated with.

Variation Justification

Non Standard Process **NStd Chem Mat Proc**
 Standard Process **Std Chem Mat Proc**

| Standard Process Children | Non Standard Process Children | Justification |
|---------------------------|-------------------------------|--|
| | Inspection | Further inspection for harardous chemicals |
| Std Anal and Appr | NStd Anal and Appr | |
| Std Bid | Std Bid | |

Reasons

☒ Legislation

☐ Others

☐ Size of Operations

☐ New Business Line

Justification

Comments

Note: Risks, controls, and audit procedures are associated with non standard (variant) processes in the normal manner. For more information, refer to Setting up Risks in Oracle Internal Controls Manager, page 4-2, Setting up Controls in Oracle Internal Controls Manager, page 4-10, and Setting up Audit Procedures in Oracle Internal Controls Manager, page 5-2.

Revising Processes in Organizations

As noted earlier, it is advantageous for an enterprise to work with standardized business processes. Though processes may be formally standardized across an enterprise, they may still differ in their execution in different organizations. This holds true even for processes that are designed as non-standard processes i.e. the non-standard process can be implemented in different ways in different organizations. The changes can exist to account for legislation, changes in the environment of the process, etc.

Note: For more information on non-standard processes, refer to Revising Processes in the Risk Library - Part 2 (Process Variation Management), page 3-12.

Rather than always creating multiple variations of a process/process hierarchy to account for these differences, Oracle Internal Controls Manager allows you to make changes to processes in individual organizations of the enterprise. The changes are unique to an organization and not reflected in others. You can therefore associate a standard process to multiple organizations and then customize (revise) each one independently. This will result in differences between processes in the risk library and the organizations they are assigned to i.e. unique exceptions to the standard process can be created in organizations.

Note: For detailed information on associating processes with organizations, refer to Organizations in Oracle Internal Controls Manager, page 2-29.

It is important to note that in order to add a risk library object to an organization, either as an addition or a replacement, the object must exist in the risk library of Oracle Internal Controls Manager.

To revise processes in Organizations

Revising organization processes is done in the Process Hierarchy Workbench (within an organizational context).

| Topic | Navigation Path |
|---|---|
| Accessing the Latest Hierarchy of Processes | Using the OICM Super User (or equivalent) responsibility, navigate to the Organizations tab and then drill into a particular organization to view the Approved Hierarchy in that organization. In the Approved Hierarchy view, click on the Modify Process icon for the appropriate process to access the "Process Hierarchy Workbench" and then drill into the appropriate process. |

You may update any and all facets of draft or previously approved processes. You can also update risk library objects associated with the org process. Select the Update drop down menu choice and then navigate to the appropriate subtab like Accounts, Risks, Controls, etc. to make any changes.

HomeAudit OperationsSegregation of DutiesOrganizationsRisk LibrarySetup

Organizations > Organization: Vision Corporation > Process Hierarchy Workbench: Vision Corporation > Process Code: NMP-Monitor Capital Project Costs > Update Process: NMP-Monitor Capital Project Costs, Vision Corporation

CancelApply

Process Name: NMP-Monitor Capital Project CostsVersion Number: 3Process Code: WM3

Basic InformationObjectivesSignificant AccountsRisks And ControlsAttachments

Select Risks (Remove)Add Risk

Select AllSelect None

| Select Name | Likelihood | Impact | Material | Material Value | Update Controls |
|---|------------|---------------|----------|----------------|-----------------|
| <input type="checkbox"/> Financial misstatement or the financial statements | Rare | insignificant | | | Update |

In the Process Hierarchy Workbench within an organization, you may also choose to "Synchronize" the process with its original in the risk library.

HomeAudit OperationsSegregation of DutiesOrganizationsRisk LibrarySetup

Organizations > Organization: Vision Corporation > Process Hierarchy Workbench: Vision Corporation > Synchronize Process: NMP-Monitor Capital Project Costs

CancelSubmit

☐ Import Risks and Controls from Risk Library Process☐ Synchronize Process

☐ Include All Sub Processes to Synchronize

Process Name: NMP-Monitor Capital Project CostsOrganization: Vision CorporationProcess Code: WM3

The options when performing this synchronization are detailed in the table below. The options can be used in combination (options 2 and 3 must be used together).

| Synchronize Option | Description |
|--|---|
| 1. Import Risks and Controls From Risk Library Process | <p>Synchronize the risks and controls of the process with those of the same process in the risk library.</p> <p>If options 2 and 3 are not used with option 1, this option can be used to synchronize only the risk and control of the individual process. Checking options 2 and 3 with option 1 synchronizes the attributes of the process (and subprocesses) and its risks and controls (as well as the risks and controls of subprocesses).</p> |
| 2. Synchronize Process | <p>Synchronize the process attributes with the attributes of the same process in the risk library.</p> |
| 3. Include All Sub Processes to Synchronize | <p>This option must be used in conjunction with Option 2. Include the subprocesses when synchronizing.</p> |

Note: Revising Sub-Processes

The initial view of the processes in an organization is from the Oracle Internal Controls Manager risk library.

Note: For more information, refer to Organizations in Oracle Internal Controls Manager, page 2-29.

You may click on the risks/controls hyperlinks to drill down to a detailed view of these objects associated with the process. If you drill down to the details pages, note the following points regarding the numbers:

- The number of risks associated with a parent process corresponds to the total of the risks attached to the child processes.
- The number of controls associated with a parent process does not necessarily correspond to the total of the children as the application displays only distinct controls in the details page.

Select the Add Sub-Process icon for the relevant process to create the revision in this organization. As noted earlier, these changes are not reflected in any other organization. You may add:

1. An existing process from the organization
2. A process from the application's risk library

In this latter case, OICM gives you the option to "Synchronize the existing subprocess" or just "Apply RCM."

Note: For detailed information on these options, refer to Linking Processes with Organizations, page 2-31.

Note the following points with respect to creating process revisions in an organization:

- The list of values for processes that you can add or replace in an organization is a subset of all processes in the process risk library. This is because the application precludes you from adding sub-processes in the hierarchy that will create circular relationships.
- Changes to process attributes within an organization, for example the process owner, are reflected in ALL occurrences of that process within the organization.

Process Revision Examples

The following examples provide more details of process revision functionality in OICM. They can also be used to understand the rules by which revision numbers are incremented. Unless otherwise stated, assume that the Approval Option parameter is set to "Approval Independent of Descendents Approval Status."

In these examples, P(A/D,1,X) denotes a Process P that has a status A-Approved or D-Draft, a revision number 1, and attribute X[n].

Process Revision Notation: The process attribute revision number is a counter associated with each process and keeps track of the number of revisions the process has undergone. When a process is first created or imported in OICM, it is given a revision number "1." Each subsequent revision results in this number being increased by one. Revision notation will not be used for the top level process ALL which is always considered to have a status of "Approved" and a revision number of "1."

Process P is an approved process (in it's second revision) with children P1 and P2 as follows:

```
P(A,2,X)
|
|--P1(A,1,X)
|
|--P2(D,1,X)
```

Example 1

Suppose attribute value X of Process P is changed to X1. Then P is now considered revised and its status changes to "Draft."

```
P(D,3,X1)
|
|--P1(A,1,X)
|
|--P2(D,1,X)
```

Example 2

Suppose we were to add a child P3 to P then the hierarchy would look like this:

```
P(D,3,X)
|
|--P1(A,1,X)
```

```

|
|--P2(D,1,X)
|
|--P3(D,1,X)

```

Suppose P is then submitted for approval and subsequently approved. The **Latest Hierarchy** now looks as follows:

```

P(A,3,X)
|
|--P1(A,1,X)
|
|--P2(D,1,X)
|
|--P3(D,1,X)

```

After this approval assume that P3 is deleted. OICM does not consider this change to be a new revision of P as revisions can only take place on approved processes. So the **Latest Hierarchy** becomes

```

P(A,3,X)
|
|--P1(A,1,X)
|
|--P2(D,1,X)

```

Note that the process revision number has not changed.

However if we deleted the process P1 (which has a previous approved revision) instead of P3, then P is considered revised. The **Latest Hierarchy** in this case is:

```

P(D,4,X)
|
|--P2(D,1,X)
|
|--P3(D,1,X)

```

Process Deletions (Removals and Disassociations)

Deleting a process in OICM takes the form of a "Removal" or "Disassociation" from the process hierarchy. Removals can be performed in the context of both risk library and organization while a Disassociation is executed for an organization only.

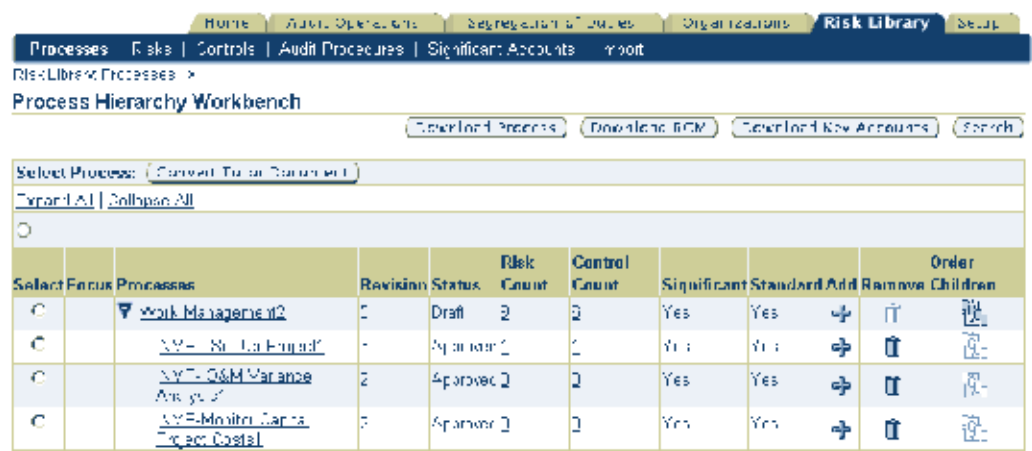
The functional difference between the two is as follows: "Remove" breaks the link between a process and it's parent (in the risk library or organization process hierarchy) while "Disassociate" removes all instances of the process from an organization's process hierarchy. In both cases the process itself remains in the system.

Both Removal and Disassociation are done in the Process Hierarchy Workbench.

Process Removal in the Risk Library

| Topic | Navigation Path |
|-----------------|--|
| Process Removal | <p>Risk Library</p> <p>Using the OICM Super User (or equivalent) responsibility, click the Risk Library tab and then the Processes subtab.</p> <p>In the Approved Hierarchy view, click on the Modify Process icon for the appropriate process to access the "Process Hierarchy Workbench" and the "Remove" icon.</p> <p>Organization</p> <p>Using the OICM Super User (or equivalent) responsibility, click the Risk Organizations tab and drill down into the details of the applicable organization.</p> <p>In the Approved Hierarchy view of processes, click on the Modify Process icon for the appropriate parent process to access the "Process Hierarchy Workbench" and the "Remove" icon.</p> |

"Remove" functionality breaks the link between a process and it's parent in the process hierarchy.



Process Disassociation in Organizations

| Topic | Navigation Path |
|---|---|
| Accessing the Latest Hierarchy of Processes | <p>Using the OICM Super User (or equivalent) responsibility, navigate to the Organizations tab and then drill into a particular organization to view the Approved Hierarchy in that organization.</p> <p>In the Approved Hierarchy view, navigate to the Modify Process icon for the appropriate process to access the "Process Hierarchy Workbench" and the "Disassociate" button.</p> |

Remember that "Disassociating" a sub-process from a particular node in the process hierarchy is equivalent to deleting that process from the organization i.e. the sub-process is detached from that particular node as well as all others in the organization. Hence

disassociating a parent process from any node of the process hierarchy in the organization removes the parent and all its sub-processes from all nodes in the hierarchy.

Process Deletion Examples

Example 1 - Removal from the Risk Library

Consider an Approved Hierarchy in the risk library as follows:

All Processes (Approved Hierarchy)

```
|
P1(A,2,X)
| |
| |----P2(A,2,X)
| |
| |----P3(A,1,X)
|
|----P3(A,1,X)
```

Suppose P3 is "Removed" as a child of P2. Then the resultant hierarchy is:

All Processes (Latest Hierarchy)

```
|
P1(D,3,X)
| |
| |----P2(A,2,X)
|
|----P3(A,1,X)
```

Note that only the instance of P3 that is a child of P2 is removed. However P3 is still within the hierarchy of P1.

The resulting Approved Hierarchy is simply "All Processes."

All Processes (Approved Hierarchy)

Example 2 - Disassociation from an Organization

Consider an Approved Hierarchy in an organization as follows:

All Processes (Approved Hierarchy)

```
|
P1(A,2,X)
| |
| |----P2(A,2,X)
| |
| |----P3(A,1,X)
```

|

P3(A,1,X)

Suppose P3 is "Disassociated" from the hierarchy. Then the resultant hierarchy is:

All Processes (Latest Hierarchy)

|

P1(D,3,X)

|

|----P2(A,2,X)

With this Disassociation, all instances of P3 are removed from the hierarchy of P1.

The new Approved Hierarchy is again:

All Processes (Approved Hierarchy)

Note that though P3 does not appear in either the Approved or Latest Hierarchies, the owner of P3 can still access and modify it as required.

Example 3

Consider a process hierarchy as follows:

P(A,3,X)

|

|--P1(A,1,X)

|

|--P2(D,1,X)

Assume that P2 is removed from the hierarchy. OICM does not consider this change to be a new revision of P as revisions can only take place on approved processes.

So the **Latest Hierarchy** becomes

P(A,3,X)

|

|--P1(A,1,X)

However if we removed the process P1 (which has a previous approved revision) instead of P2, then P is considered revised. The **Latest Hierarchy** is now:

P(D,4,X)

|

|--P2(D,1,X)

Submitting Processes and Process Revisions for Approval

Once the modification of processes is complete, you are ready to approve/submit the process.

Setup for Process Approval

The steps to setup the Oracle Internal Controls Manager application for process approval are listed below:

1. Create the process approval templates
2. Seed these templates as the active process approval routing templates within OICM

Create the Process Approval Templates

There are two workflow templates that must be setup for the approval of processes:

- The Process Approval Template: Applies to process approvals in the OICM Risk Library
- The Organization Process Approval Template: Applies to process approvals in all organizations

The following discussion pertains to the Process Approval Template.

Note: The creation of the Organization Process Approval Template is a mirror of this setup.

| Topic | Navigation Path |
|--|--|
| Setting up the Process Approval Template | Using the OICM Super User (or equivalent) responsibility, click the Setup tab and then the Approvals subtab. Drill down into "Approval Templates" to access the "Process Approval" Template (and "Organization Process Approval" Template). Drill into this template to view its details. |

You may use the seeded template or duplicate and modify the same (click the Update button).

[Home](#) | [Alert Operations](#) | [Sequencing of Duties](#) | [Organizations](#) | [Risk Library](#) | **Setup**

[Request Approval](#) | [Request Management](#) | [Options](#) | [Risk Library](#) | [Regulators](#) | [Approvals](#) | [Value Stream](#)

[Setup Approvals](#) > [Workflow Templates](#) >

Update Workflow Template

* indicates required field

Name:

Description:

Start Date:

End Date:

Type:

| Details | Step | Workflow Process | Response Required | Type | Assigned To | Days to Respond | Update | Delete |
|-------------------------|----------------------------|------------------|-------------------|---------|--------------------------------------|-----------------|------------------------|------------------------|
| Show ID | Request Approval Options | | Any Response | Process | Risk Library Process Owner | | Update | Delete |
| Show ID | Request Approval Mandatory | | Any Response | Process | Risk Library Process Change Approver | | Update | Delete |

Process approvals using the seeded "Process Approval Template" takes the following form:

- Approval is optional from the owner/owners of this process in the Risk Library. These individuals are those who are assigned a "Risk Library Process Owner" role on the process.
- Approval is mandatory from change approvers of the process in the Risk Library. These individuals are those who are assigned a "Risk Library Process Change Approver" role on the process.

Once the workflow successfully traverses a particular step it then advances to the requirements of the next step. You can modify almost all facets of the workflow template. For example, in a particular workflow step you can change the list of assignees, whether an approval is required from "One Assignee"/"All Assignees"/"Mandatory Assignees," the "Days to Respond", etc.

Setup: Approvals >

Update Step: 10

no steps required field [Cancel] [Add Assignee] [Apply]

Step: 10

Workflow Process: Request Approval

Assignee: Derive

Response Required: Mandatory Assignees

Days to Respond: All Assignees

Instructions: Mandatory Assignees

Assignees

Add Assignee Role [Add]

| Type | Name | Company | Response Required | Delete |
|----------------------|--------------------------------------|---------|-------------------|--------|
| Appx RL Process Role | Risk Library Process Change Approver | | Mandatory | [X] |
| Appx RL Process Role | Risk Library Process Owner | | Optional | [X] |

Note: You may modify the seeded template as appropriate. For more information on setting up workflows, refer to the *Oracle Workflow Guides*.

Seed the Process Approval Templates in OICM

Perform the following two steps to seed the templates as the active process approval routing template within OICM:

1: Access the workflow for the Risk Library Process Approval Category and the Process (Risk Library) Type. In the case of organization process approvals, access the Organization Process Approval Category and the Process (Organization) Type.

Note: The Process Approval (Risk Library) Type and the Process Approval (Organization) Type are for internal use only.

First access the Process Approval (or Org Process Approval) Type within OICM

| Topic | Navigation Path |
|--|---|
| Seed Workflow Approval Templates in OICM | <p>Using the OICM Super User (or equivalent) responsibility, click the Setup tab and then the Issues Management subtab. Drill down into "Categories and Type" to access the Risk Library Process Approval (and Organization Process Approval) Categories.</p> <p>For the Risk Library Process Approval Category (or Organization Process Approval Category), navigate to the Type subtab.</p> |

Home Audit Operations Segregation of Duties Organizations Risk Library Setup

Engagements | **Issue Management** | Opinions | Risk Library | Regulations | Approvals | Value Sets

Setup: Issue Management >

Categories

Select Category: Duplicate Update Previous 5 6-9 of 9 Next

| Select | Name | Description | Created By | Start Date | End Date | Search Criteria | Display Format |
|----------------------------------|-------------------------------|-------------------------------|----------------|-------------|----------|-----------------|----------------|
| <input type="radio"/> | Sign Off Request | Sign Off Request | Richard Abbott | 11-Feb-2005 | | | |
| <input type="radio"/> | Incident | Incident | Richard Abbott | 27-Oct-2004 | | | |
| <input checked="" type="radio"/> | Risk Library Process Approval | Risk Library Process Approval | Richard Abbott | 11-Feb-2005 | | | |
| <input type="radio"/> | Organization Process Approval | Organization Process Approval | Richard Abbott | 11-Feb-2005 | | | |

Category: Risk Library Process Approval

Basic Information Types Line Types Reports

Select Header Type: Duplicate Update Create

| Select | Name | Description | Subject Type | Created By | Start Date | End Date |
|----------------------------------|---------------------------------|---------------------------------|-----------------------|----------------|-------------|----------|
| <input checked="" type="radio"/> | Process (Risk Library) | Process (Risk Library) | AMW_REVISION_ETTY | Richard Abbott | 11-Feb-2005 | |
| <input type="radio"/> | Process Approval (Risk Library) | Process Approval (Risk Library) | AMW_PROCESS_APPR_ETTY | Richard Abbott | 11-Feb-2005 | |

2: Modify the workflow

Drill down into the Process (Risk Library) Type to access the process approval Workflow. In the case of organization processes, drill down into the or the Process (Organization) Type.

Home Audit Operations Segregation of Duties Organizations Risk Library Setup

Engagements | Issue Management | **Workflow** | Opinions | Risk Library | Regulations | Approvals | Value Sets

Basic Information Attribute Groups Pages Codes Configuration **Workflow**

Workflow

Change Category: Risk Library Process Approval

Cancel Apply

Type: Process (Risk Library)

Select Status: Delete

| Select | #Number | #Status | Status Type | Update Properties |
|----------------------------------|---------|-----------|-------------|-------------------|
| <input checked="" type="radio"/> | 01 | Approval | Approval | |
| <input type="radio"/> | 02 | Completed | Implemented | |

Add Another Row

For the appropriate workflow step, click the Update Properties icon to seed the Process Approval Template (created earlier) for that step. Process Approval Templates must be seeded for each step i.e. for each change of status.

As an example, consider a workflow with two phases - "Approval" and "Completed." The workflow routing (based on the template that is created in point 1 and seeded for this status) must be entirely traversed to change the status of the submitted process from "Approval" to "Completed."

Note: The remaining setups (like Attribute Groups, Pages, etc.), mirror those described in the chapter Findings in Oracle Internal Controls Manager.

Enable Business Event Processing

Process approvals utilizes business events in its functioning. It is critical to confirm that events handling the approvals are enabled.

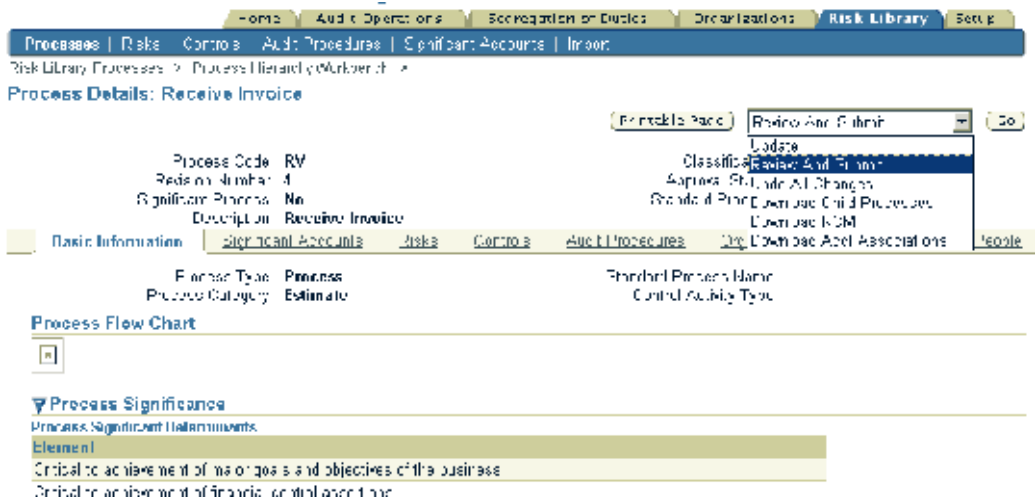
Perform the following task in Oracle Workflow:

| Topic | Navigation Path |
|--|---|
| Enable the Process Approval Business Event | <p>Using the Workflow Administrator Web Applications (or equivalent) responsibility, navigate to the Administrator Workflow and then the Business Events domain.</p> <p>Now search for the "oracle.apps.eng.cm.changeObject.changeApprovalStatus" event [Events Window].</p> <p>Subsequently, drill into the event by clicking the Update icon [Update Event Window] and ensure that its status is "Enabled."</p> |

If necessary, change the Status of the Event's subscription to Enabled. Note that to execute this task you must be logged in as a System Administrator or user with Update privileges.

Submit the Process for Approval

Once all changes are made in the Process Hierarchy Workbench, you can submit the process for approval (Organization process approval is a mirror of this submission).



Note: If Auto Approval is set to Yes, then the "Publish" option (instead of "Review and Submit") is available and the process is automatically approved.

Once submitted, the application displays a summary window where users can review what changes were made to the process and decide whether to continue with the submission. Changes take the following three forms:

- Modification of process or associated risk library object values

- Addition of risk library objects associated with the process
- Deletion of risk library objects associated with the process

Standard Process: Receive Invoice
Revision Number: 4

Process Code: RV
Description: Receive Invoice

Process Attributes Modification Summary

| Attribute | Old Value | New Value |
|---------------------|-----------|-----------|
| Process Category | Routine | Estimate |
| Significant Process | Yes | No |

Risks Modification Summary

| Risk Name | Modification Type | Likelihood | Impact | Material | Material Value | Approval Status |
|-----------|-------------------|------------|--------|----------|----------------|-----------------|
| Bed Crac | Add | Rare | Major | No | | Draft |
| Bed Crac | Delete | Unlikely | Major | No | | Draft |

Finally, review the parameters of the Change Request (workflow, Pages, Dependencies, Attribute Groups, etc.) that are created according to the Process Approvals setups described earlier in this section and Submit for approval.

Note: For more details on these Change Request parameters, refer to Findings in Oracle Internal Controls Manager, page 12-1.

Change Request Type: Process (Risk Library)
Change Request Number: PROCRL16
Change Request Name: Proc16
Description: [Text Area]

Process Name: Receive Invoice
Process Code: RV
Process Number: 4

Additional Information

Assign To: [Text Field]
Priority: High
Reason: Fraud
Requester: [Text Field]
Request Date: [Text Field]

Process History

Modification of a process in OICM results in a process revision. However, older versions remain in the system and you can at any point in time view prior revisions of the process as a part of the history of the process.

| Topic | Navigation Path |
|--|---|
| View the history of revisions of a process | Using the OICM Super User (or equivalent) responsibility, click the Risk Library tab and then the Processes subtab to view the Approved Hierarchy. Alternately, navigate to the Organizations tab and drill into a particular organization to view the Approved Hierarchy in that organization. In the Approved Hierarchy view, drill into the details of the appropriate process to access the "History" tab. |

HomeAudit OperationsSegregation of DutiesOrganizationsRisk LibrarySetup

Processes | Risk ControlsAudit Procedures | Significant Accounts | Import

Back to Main Processes +

Process Details: Receive Invoice

Printable Page

This Process is being revised. Latest Revision: 2

Process Code: RV

Revision Number: 4200

Significant Process: No

Classification: SOX

Approval Status: Approved

Control Process: Yes

Description: Narrative Invoice

Basic InformationSignificant AccountsRisksControlsAudit ProceduresOperationsAttachmentsPeopleHistory

Process Revisions

| Select | Revision Number | Start Date | End Date | Intermediate Date | Change Request |
|-----------------------|-----------------|---------------------|---------------------|---------------------|----------------|
| <input type="radio"/> | 1 | 2005-04-11 10:00:00 | 2005-04-11 10:00:00 | 2005-04-11 10:00:00 | 1000 |
| <input type="radio"/> | 2 | 2005-04-11 10:00:00 | 2005-04-11 10:00:00 | 2005-04-11 10:00:00 | 1000 |
| <input type="radio"/> | 3 | 2005-04-11 10:00:00 | 2005-04-11 10:00:00 | 2005-04-11 10:00:00 | 1000 |
| <input type="radio"/> | 4 | 2005-04-11 10:00:00 | | | 1000 |

Process Hierarchy

Expand Collapse All

| Process Name | Process Code | Num of Controls | Num of Risks |
|-----------------|--------------|-----------------|--------------|
| Receive Invoice | RV | | |

Process Revision Number and Process Hierarchy Links

Click on the Process Revision Number to view the detailed settings of the process for that revision.

Note that the history of a process involves not only the changes in its attributes and associated risk library objects but also changes in its hierarchy. Hence each revision corresponds to a Process Hierarchy link where you can view the details of the active hierarchy for that revision.

Intermediate Date

Hierarchy changes in a process beyond the first level of children do not result in a process revision. However you can view the detailed hierarchy at any date between the Start and End date of the revision by entering a date in the "Intermediate Date" field.

Risks and Controls in Oracle Internal Controls Manager

This chapter covers the following topics:

- Overview of the Risk Library
- Risks
- Controls
- Importing Risks and Controls into Oracle Internal Controls Manager
- Export Risk and Control Objects

Overview of the Risk Library

The risk library consists of processes and process risks, as well as the policies, procedures, and activities that allow an organization to address those risks. There are four primary objects in the risk library:

- Processes
- Risks
- Controls
- Audit Procedures

The library is therefore analogous to a container that holds these objects for all organizations in the enterprise. Multiple libraries are not allowed.

A risk library can consist of content from professional organizations (for example, The Institute of Internal Auditors or Accounting Firms), and/or from users in the organization. If you decide to implement a partner's library, Oracle Internal Controls Manager includes a spreadsheet interface that allows third party content to be imported.

Note: For more information on importing risk library objects into Oracle Internal Controls Manager, refer to Importing Risks and Controls into Oracle Internal Controls Manager, page 4-17.

Processes are fully described under Processes in Oracle Internal Controls Manager and Audit Procedures under Audit Procedures in Internal Controls Manager.

Risks

Risks are defined as the possibility of acts or events occurring that would have an adverse effect on the organization's processes and its control environment. An example of a risk would be having the same person who enters supplier information into the system also enter and pay invoices.

The Risks tab allows you to change the orientation of your information from being centered around the processes in the organization to being centered around the risks to which the processes are exposed.

Auditors identify the risks associated with each business process and organization and the possible effects they might have. Use Oracle Internal Controls Manager to create and maintain a library of reusable risks that can then be associated with business processes or "entities." Entity Risks are risks that are directly linked with organizations. For example the risk that users may not be adequately trained is more appropriately tied to an organization. All risks can be classified for their probability and impact. For example, the risk that a loss resulting order is accepted may be a low probability risk that has a high impact.

Setting up Risks in Oracle Internal Controls Manager

Oracle Internal Controls Manager allows you to create risks in two ways:

1. Use the following menu path to manually create your risks.

| Topic | Navigation Path |
|---|---|
| To create a Risk in the OICM Risk Library | Using the Internal Auditor (or equivalent) responsibility, click the Risk Library tab. In the Risks subtab section, click the Create button. |

Note: For more information on select fields in the Risks Details page, refer to the sections below on Risk Attributes, page 4-4 as well as the sections on Risks, Risk Types and Regulations, page 4-5.

If you save the risk for later editing, the risk is created with a status of "Draft." When the risk is finalized, click on Update in the main Risks page (in the Risk Library) and then submit the risk for approval. If you need to update an approved risk, drill into the risk details and then select Revise.

Note that risk library objects can only be utilized in Oracle Internal Controls Manager after they are approved. Risks are approved/reapproved based on your setup of workflow rules and the approval hierarchy in the Oracle Approvals Management application. When the approval is complete, the risk approval status changes to Approved.

Note: The use of Oracle Approvals Management for approving risk library objects is optional. For more details, refer to Risk Library Change Control, page 6-1.

To manually link the risk with other objects like processes and organizations, use the following menu path:

| Topic | Navigation Path |
|--|--|
| Manually associate Risks with Organizations, Processes, and Controls | <p>To Link the Risk with Organizations:</p> <p>Using the internal auditor (or equivalent) responsibility, click the Organization tab and then drill down into the appropriate org.</p> <p>In the Org details view, navigate to the Risks subtab to link the risk with the org.</p> <p>To Link the Risk with Processes and Controls:</p> <p>Using the internal auditor (or equivalent) responsibility, click the Organization tab and then drill down into the appropriate org.</p> <p>From the Process subtab view, navigate to the Process Hierarchy Workbench (by clicking the Modify Process icon for the appropriate process). Drill into a Process in this workbench window and then click the Risks subtab.</p> <p>In this details view, click the Update button and then navigate to the 'Risks and Controls' subtab. You can Add Risks as well as associate Controls with the Process Risks.</p> |

2. Import Risks from the Setup tab. Instead of creating risks manually and then associating them with controls and with processes individually, Oracle Internal Controls Manager provides a powerful import mechanism for risk and control objects. Using this import functionality you can import risks and controls and associate them with processes and organizations in a single step.

Note: For more information, refer to the section Importing Risks and Controls into Oracle Internal Controls Manager, page 4-17

Risk Attributes

Home | Add | Configuration | Setup | Information | Outlets | Organization | Risk Library | Sign up

Processes | **Risks** | Controls | Audit Procedures | Impact

[Risk Library Page](#)

Create Risk

Indicates required field

Risk Name

Classification

Description

Material

Cancel Save for Later Submit

Severity

Impact

Risk Types

[Select All](#) | [Select None](#) | [Expand All](#) | [Collapse All](#)

| Select | Focus | Name | Description |
|--------------------------|-------------------------------------|----------------------------------|------------------------|
| <input type="checkbox"/> | | Root Risk Type | Uncontrolled risk type |
| <input type="checkbox"/> | | ADW Training | ADW Training |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | Internal Fraud | |
| <input type="checkbox"/> | | Unauthorized Activity | |
| <input type="checkbox"/> | | Internal Fraud - Theft and Fraud | |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | External Fraud | |
| <input type="checkbox"/> | | External Fraud - Theft and Fraud | |
| <input type="checkbox"/> | | System Security | |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | Employment Practices | |
| <input type="checkbox"/> | | Employment Practices | |
| <input type="checkbox"/> | | Performance | |

The following table provides further information on select fields in the Risk details and Results pages.

| Field | Details | Seeded Values | Lookup Type | Accessibility Level |
|-----------------|---|---|--------------------------------------|---------------------|
| Classification | Determines the extensible attributes displayed for the risk. For more information, refer to Extensible Attributes, page 14-1 | NA | NA | NA |
| Likelihood | User defined risk classification | Rare Unlikely Often Most Time Certain | AMW LIKEL IHOOD | User |
| Impact | User defined risk classification | Insignificant Minor Moderate Major Catastrophic | AMW IM PACT | User |
| Approval Status | The Approval Status of the Risk. To be available for use in Oracle Internal Controls Manager, a Risk must have a status of "Approved" | Approved Draft Pending Approval Rejected | AMW_R ISK_AP PROVAL_ STATUS | System |
| Material | Would the damage or loss be material if the risk occurred | Yes No | N/A | N/A |
| Risk Type | User defined risk classification. You can associate multiple risk types with a risk. For more information refer to the section Risks, Risk Types and Regulations, page 4-5. | NA | NA | NA |

Risks, Risk Types and Regulations

Risks and Risk Type

To facilitate Basel II requirements, Risks and Processes need to be classified as belonging to appropriate Regulations (Regulatory Environments).

Note: For more information on Regulations and their creation, refer to the White Paper "Integration with Oracle's Basel II Solution".

Risks are classified by Risk Type and a risk in the OICM risk library is associated with one or more Regulations through the use of its Risk Type. Risk Types are seeded within the OICM library that are compliant with the Sarbanes Oxley and Basel II operational risk frameworks.

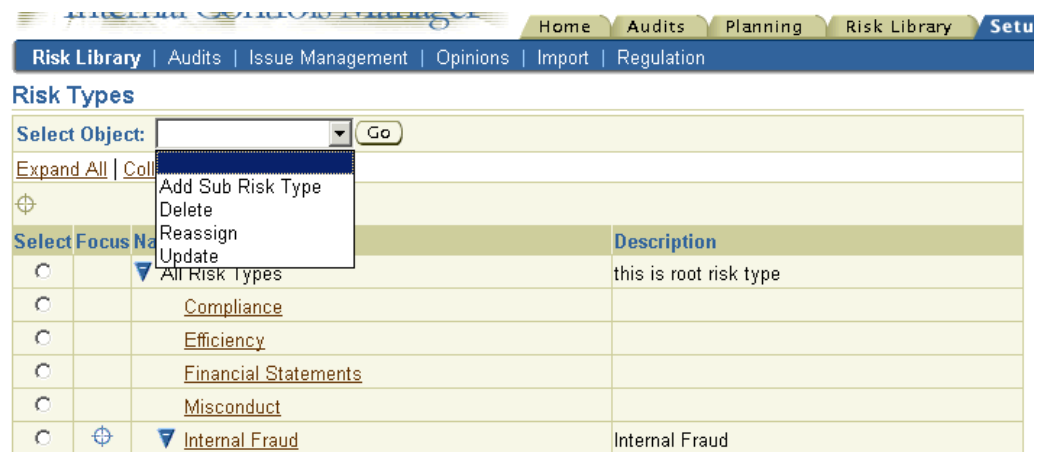
The following list shows the Level I and Level II Risk Types that are seeded in OICM for Basel II:

| Type (Level 1) | Definition | Type (Level 2) with Examples |
|---|---|---|
| Internal Fraud | Losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy, excluding diversity/discrimination events, which involves at least one internal party | Unauthorized Activity (Transactions not reported - Intentional, Transaction type unauthorized - with monetary loss) Theft and Fraud (Credit fraud / theft / extortion / embezzlement, Misappropriation of Assets, Malicious destruction of assets Bribes / kickbacks) |
| External Fraud | Losses due to acts of a type intended to defraud, misappropriate property or circumvent the law, by a third party | Theft and Fraud (Theft, forgery) Systems Security (Hacking damage, theft of information) |
| Employment Practices and Workplace Safety | Losses arising from acts inconsistent with employment, health or safety laws or agreements, from payment of personal injury claims, or from diversity / discrimination events | Employee Relations (Compensation, benefit, termination issues) Safe Environment (General liability Employee health and safety) Diversity and Discrimination (Workers compensation, All discrimination types) |
| Clients, Products, and Business Practices | Losses arising from an unintentional or negligent failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements), or from the nature or design of a product | Suitability, Disclosure and Fiduciary (Disclosure issues, aggressive sales) Improper Business or Market Practices (Antitrust, insider trading, unlicensed activity) Product Flaws (Product defects) Selection, Sponsorship, and Exposure (Failure to investigate client per guidelines) Advisory Activities (Disputes over performance of advisory activities) |
| Damage to Physical Assets | Losses arising from the loss or damage to physical assets from natural disaster or other events | Disasters and other events (Natural disaster losses) |
| Business Disruption and System Failures | Losses arising from disruption of business or system failures | Systems (Hardware, software, telecommunications) |
| Execution, Delivery, and Process Management | Losses from failed transaction processing or process management, from relations with trade counterparts and vendors | Transaction Capture, Execution and Maintenance (Data entry/loading errors, accounting errors) Monitoring and Reporting (Inaccurate report-external) Customer Documentation (Legal documents missing) Customer / Client Account Management (Unapproved access given to accounts, Miscellaneous non-client disputes) Trade Counterparts / Vendors and Suppliers (Vendor disputes) |

Organizations may add to this embedded library of Risk Types to include other risks as follows:

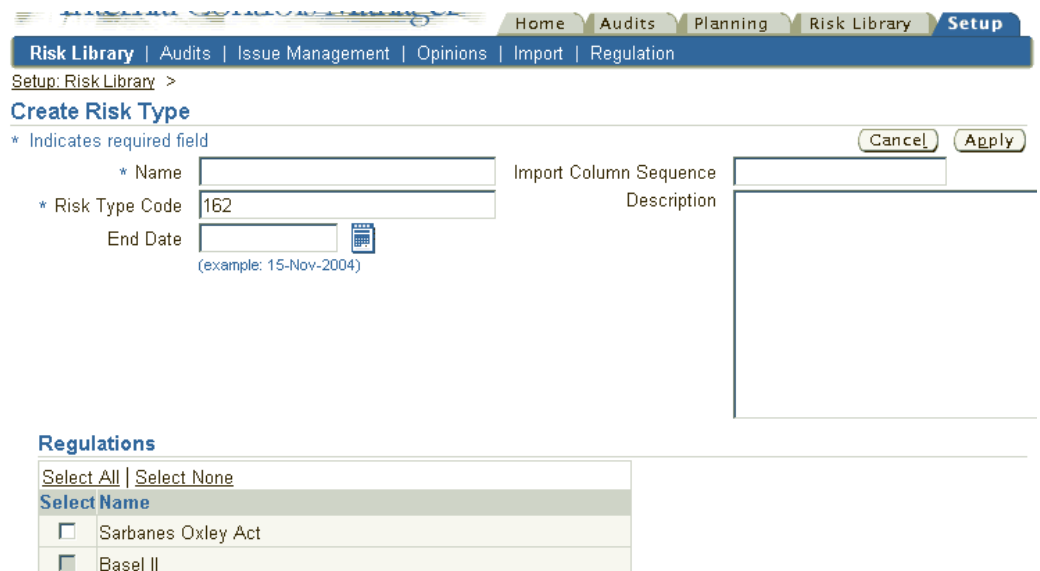
To Create a Risk Type

| Topic | Navigation Path |
|---------------------|---|
| Defining Risk Types | <p>Using the Internal Auditor (or equivalent) responsibility, click the Setup tab and then the Risk Library subtab.</p> <p>Drill down into the Risk Types link.</p> <p>To create a Level I Risk Type, click the "All Risk Types" option and then select "Add Sub Risk Type" from the drop down menu.</p> <p>To create a subsidiary level Risk Type, click the parent Risk Type then select "Add Sub Risk Type" from the drop down menu.</p> |



| Select | Focus | Name | Description |
|-----------------------|----------------------------------|----------------------|------------------------|
| <input type="radio"/> | | All Risk Types | this is root risk type |
| <input type="radio"/> | | Compliance | |
| <input type="radio"/> | | Efficiency | |
| <input type="radio"/> | | Financial Statements | |
| <input type="radio"/> | | Misconduct | |
| <input type="radio"/> | <input checked="" type="radio"/> | Internal Fraud | Internal Fraud |

You can also Delete, Reassign, and Update Risk Types in this window. Note that there is no limit to the number of Risk Types or Risk Type levels.



Create Risk Type

* Indicates required field

* Name: Import Column Sequence:

* Risk Type Code: Description:

End Date: (example: 15-Nov-2004)

Regulations

Select All | Select None

Select Name

☐ Sarbanes Oxley Act

☒ Basel II

When creating Risk Types, map them to appropriate Regulations.

The following table provides further information on select fields in the Create Risk Type window.

| Field | Details | Seeded Values |
|------------------------|--|-------------------------------|
| Risk Type Code | Unique identifier for the Risk Type. A sequentially generated number is automatically defaulted, but can be changed by the user. Once the Risk Type is created, you cannot update the Risk Type Code. | Sequentially generated number |
| Import Column Sequence | Column sequence number for the Web ADI upload. Upto 30 Risk Types can be imported through the spreadsheet upload. | N/A |
| Regulations | See the Risk Types and Regulations section below | NA |

Risk Types and Regulations

As noted earlier, Risks and Processes need to be classified as belonging to appropriate Regulations (Regulatory Environments) in order to meet Basel II requirements. This is done in the following way:

1. When a Risk is created, it is classified as having one or more Risk Types.

Note: For more details, refer to the section Risk Attributes., page 4-4

2. The Risk Type, when created, is mapped in turn to one or more Regulations. Different Regulations can therefore have different sets of Risk Types. For example, the SOX Regulation can have one set of Risk Types while the Basel II Regulation has a different set. Overlap is allowed and a particular Risk Type can be used by multiple Regulations.

Note: The only Regulations available when mapping a new subsidiary Risk Type to a Regulation are those associated with the parent Risk Type i.e. you can only map the subsidiary Risk Type to a Regulation that is also associated with the parent.

Similarly, a subsidiary Risk Type can only be reassigned to other Risk Types that are linked with the same Regulation as the original parent.

As a result of the mapping between the Risk, Risk Type, and Regulation, the created Risk is now associated with Risk Types within specific Regulations.

[Home](#)
[Audits](#)
[Planning](#)
[Risk Library](#)

[Processes](#)
[Risks](#)
[Controls](#)
[Audit Procedures](#)

[Risk Library: Risks](#) >

Risk Details: Fraudulent Returns

This risk is being changed: Revision **6**

| | | | |
|------------|---------------------------|----------|--------------|
| Risk Name | Fraudulent Returns | Impact | Major |
| Likelihood | Often | Material | Yes |

[Basic Information](#)
[Processes](#)
[Controls](#)
[Objectives](#)
[Attachments](#)
[History](#)

Risk

| | | | |
|---------------|---------------------------|-----------------|--------------------|
| Description | Fraudulent Returns | Approval Status | Approved |
| Approval Date | 28-Apr-2004 | End Date | 28-Apr-2004 |

▼ Risk Types for Sarbanes Oxley Act

[Select All](#) | [Select None](#) | [Expand All](#) | [Collapse All](#)

| Select | Focus | Name | Description |
|-------------------------------------|-------|----------------------|------------------------|
| <input type="checkbox"/> | ▼ | All Risk Types | this is root risk type |
| <input type="checkbox"/> | | Compliance | |
| <input checked="" type="checkbox"/> | | Efficiency | |
| <input checked="" type="checkbox"/> | | Financial Statements | |
| <input checked="" type="checkbox"/> | | Misconduct | |

► Risk Types for Basel II

Note that if there are no Risk Types associated with a particular Regulation, then the application does not display that Regulation when viewing the Risk.

Risks Search

A simple search can result in your risks being listed several times, once for every process and / or organization it is associated with.

You can optionally search for a subset of risks using the following dimensions:

- Risk Name.
- Revision. For more information, refer to Revising Objects in the Risk Library, page 6-3.
- Risk Likelihood. For more information, refer to the section on Risk Attributes, page 4-4.
- Search Context (accessed via the Advanced Search button). Three search contexts are available as follows:
 - The Risks Context search returns all risks in the system without their associated process or organization names.
 - The Associated Process Context search returns all risks in the system that are associated with processes. Note that if a risk is associated with multiple processes or the same process in multiple organizations, then the risk will be listed more than once.
 - The Organization Context search returns all risks associated with organizations (through processes in those organizations).

Risk Views

You can view Risk objects in the context of both Risk Library and Organization.

| Topic | Navigation Path |
|---------------|---|
| Viewing Risks | <p>To View Risks in the Risk Library:</p> <p>Using a super user (or equivalent) responsibility, click the Risk Library tab and then the Risks subtab.</p> <p>To View Risks in their Organizational Context:</p> <p>Using a super user (or equivalent) responsibility, click the Organization tab and then drill down into the appropriate org. Under the Risks subtab you can view risks both Entity Risks and Process Risk. Entity Risks are risks that directly bear on the organization. The Process Risks are risks that the processes in this organization are exposed to.</p> |

Controls

Company management plans, organizes, and directs the performance of sufficient actions to provide reasonable assurance that the firm's objectives and goals will be achieved. Controls are actions taken by management, the board of directors, and other parties to enhance risk management and increase the likelihood that established objectives and goals will be achieved.

The Controls tab allows you to change the orientation of your information from being centered around processes or other library objects in the organization to being centered around the control objects.

Design controls to mitigate process risk. As an example, if the risk is having the same person who enters suppliers also enter and pay invoices, then an example of a mitigating control would be to split the tasks or have someone review the payment register for unauthorized supplier payments. Monthly reconciliations, credit approvals before shipment occurs and separation of duties between billing, recording sales, and handling cash receipts are examples of controls for sales transactions.

Setting up Controls in Oracle Internal Controls Manager

Oracle Internal Controls Manager allows you to create Controls in two ways:

1. Use the following menu path to manually create your controls.

| Topic | Navigation Path |
|---|---|
| To manually create a control in the OICM Risk Library | <p>Using the Internal Auditor (or equivalent) responsibility, click the Risk Library tab.</p> <p>In the Controls subtab section, click the Create button.</p> |

Note: For more information on select fields in the Control details page, refer to the sections on Control Attributes, page 4-11.

If you save the control for later editing, the control is created with a status of "Draft." When the control is finalized, click on Update in the main Controls page and then submit the control for approval. If you need to update an approved control, drill into the control details and then select Revise.

Note that risk library objects can only be utilized in Oracle Internal Controls Manager after they are approved. Risks are approved/reapproved based on your setup of workflow rules and the approval hierarchy in the Oracle Approvals Management application. When the approval is complete, the control approval status changes to Approved.

Note: The use of Oracle Approvals Management for approving risk library objects is optional. For more details, refer to Manage the Process Risk Library, page 6-1.

To manually link the control with entity and process risk, use the following menu path:

| Topic | Navigation Path | Oracle Internal Controls Manager Window |
|--|--|---|
| Manually associate Controls with Entity and Process Risk | <p>To Link the Control with Entity Risks:</p> <p>Using an Internal Auditor (or equivalent) responsibility, click the Organization tab and then drill down into the appropriate org. In the Org Details view, navigate to the Risks subtab and click Update Entity Risks.</p> <p>In the Update Entity Risks window, select the icon to Update Controls for the particular risk.</p> <p>To Link the Controls with Process Risks:</p> <p>Using a super user (or equivalent) responsibility, click the Organization tab and then drill down into the appropriate organization. From the Processes subtab, navigate to the Process Hierarchy Workbench (by clicking the Modify Process icon for the appropriate process). Drill into a Process in this workbench window and then click the Risks subtab.</p> <p>In this details view, click the Update button and then the 'Risks and Controls' subtab. In this window you can associate Controls with the Process Risks.</p> | Import Details |

2. Import Risks from the Setup tab. Instead of creating controls manually and then associating them with controls and with processes individually, Oracle Internal Controls Manager provides a powerful import mechanism for risk and control objects. Using this import functionality you can import risks and controls and associate them with processes and organizations in a single step.

Note: For more information, refer to Importing Risks and Controls into Oracle Internal Controls Manager, page 4-17

You can view all entered controls in the main Risks page by navigating to the Risk Library > Risks sub-tab.

Control Attributes

Controls have several attributes that provide more details on how a particular control is implemented in Oracle Internal Controls Manager.

The screenshot shows the 'Create Control' form in the Oracle Internal Controls Manager. The form is organized into several sections:

- Control Information:** Includes fields for 'Control Name', 'Physical Evidence', 'Classification' (set to 'Internal Control Attribute'), 'Control Type' (set to 'Policy'), 'Automation Type', 'Application', 'Control Owner', 'Unit of Measure', 'Control Frequency', and 'Description'.
- Control Location:** Includes fields for 'Control Location', 'Job Title', and 'End Date'.
- Verification Mechanism:** Includes fields for 'Verification Source', 'Verification Source Date', and 'Verification Instruction'.

Buttons for 'Cancel', 'Page for Entry', and 'Submit' are located at the top right of the form.

The following sections provide more details on select attributes.

Physical Evidence

The physical evidence that should be provided if the control is a manual control, such as a physical signature from approver

Control Classification

Determines the extensible attributes displayed for the control.

For more information, refer to Extensible Attributes, page 14-1

Control Type

Lookup Type: AMW CONTROL TYPE

User Accessibility level: Extensible

The Control Type designates whether the control is inherently Automatic, Manual, a Combination of the prior two, or a Policy

| Seeded Values | Description |
|---------------|---|
| Automatic | Profiles, Application Access, Workflows, KPIs are examples of Automatic controls. These controls are enforced within the E-Business suite. |
| Combination | Alerts are an example of controls that use a combination of both automatic and manual procedures. The Alert can automatically raise a flag when a condition is met and then manual intervention is initiated. |
| Manual | Manual procedures |
| Policy | Typically controls in the form of high level business policies that are implemented across the organization. |

Automation Type, Application, and Control Source

Lookup Type: AMW AUTOMATION TYPE

User Accessibility level: System

If the Control Type is Automatic or Combination, then select the control's Automation Type. The Automation Type provides details on the kind of automatic control used to mitigate process risk.

Based on the value selected in the Automation Type field, select a corresponding Control Source. Control Sources are the names (values) of the automatic controls. For any given Automation Type, you can have a large number of corresponding control source values. For example, the Automation type "Profile" has potentially hundreds of profile values seeded in the Oracle E-Business Suite.

The Application field allows you to restrict the values in the Controls Source list of values. Once you link an Application with the Automation Type, the Control Source values are limited to those values in the selected Application.

| Seeded Values | Control is implemented through: | Control Source Values |
|--------------------|---|--|
| Profiles | Profile options and registered application parameters | All system profile option values |
| Setup | No current functionality | No control source |
| Application Access | Restricted application access | Form Functions |
| System Access | Restricted system access | No control source |
| Change Control | Controls defined in Oracle Internal Controls Manager | No control source |
| Workflow | Registered workflow activities in the application | All registered workflows |
| Alert | Alert notifications | No control source |
| Report | Applications reports | All reports in the system |
| Built In | Oracle Applications | No control source |
| KPI | KPIs in the E-Business Suite modules or the Oracle Performance Management Framework. You can set process control limits that notify you when the limits are exceeded. | All available KPIs from the Performance Management Framework |
| Manual | Manual procedures | No control source |

Unit of Measure

This is the base measure of the subsequent Control Frequency field. Typical base measures will be "Days," "Weeks," "Quarters," etc. The LOV displays values according to the profile option AMW: Unit of Measure Class for Control Frequency

Control Frequency

Denotes how often the control is executed / implemented

Disclosure vs. Key Control

Identify the control as a disclosure and/or a key control.

Companies devise and maintain a system of key internal accounting controls to ensure that financial transactions are valid, properly authorized and complete (so financial statements can be prepared in accordance with GAAP). Auditors focus primarily on the key internal controls that are of a financial nature.

Disclosure controls and procedures on the other hand are more geared towards ensuring that information required to be disclosed in financial statements and filings is properly recorded, classified, processed, and reported on a timely basis.

However, in implementing Sarbanes-Oxley laws in the USA, the SEC has deliberately defined disclosure controls to encompass more than the limited concept of internal controls. Hence, in addition to the traditional measures, disclosure controls include all systems necessary for the full, timely disclosure of all areas of operations in the

company's financial reports. The SEC explicitly includes procedures designed to ensure that the company timely collects and communicates reportable information to management. The disclosure control system should also integrate the company's internal controls and any other protective programs in the company.

Preventive vs. Detective Controls

Select whether the control is one or more of the following:

- Preventive Control
- Detective Control

Verification Mechanism

The verification mechanism allows auditors to record the verification of control settings in Oracle E-Business suite apps. Verification ensures that the current settings yield an appropriate level of control.

An example of a control setting is the "Match Type" setting in accounts payable.

- A company could run its enterprise or its operating unit with matching turned off. It might choose to enforce that Invoices must have a matching purchase order.
- It might choose to enforce that the invoices have both a matching purchase order and receipt.
- It might choose to enforce that invoices have a matching purchase order and a receipt that has been quality assured.

A control setting could be verified by:

- Automatically through a named function
- Manually through a named User Interface
- Manually through reviewing a report.

Internal Control Components

These are predefined components affecting the organization's audit environment. The seeded components shown below are from the COSO framework. You may classify the control as belonging to one of these domains.

- Control Activities
- Internal Environment
- Event Identification
- Information and Communication
- Monitoring
- Objective Setting
- Risk Assessment
- Risk Response

Note: For more information on these components, see *Creating an Assessment in Oracle Internal Controls Manager*.

Control Purposes

A taxonomy of the purpose of the control

- Initiating
- Processing
- Recording
- Reporting

Control Assertions and Objectives

The framework used to evaluate the controls that mitigate process and account balance risk includes:

- Control Assertions
- Control Objectives (also called Control Categories in the application)

Accordingly, for each control, Oracle Internal Controls Manager allows you to assign objectives and assertions.

a. Control Assertions

Lookup Type: AMW CONTROL ASSERTIONS

Accessibility Level: Extensible

Assertions refer to implied or expressed representations by management about an organization's processes and/or the components of its financial statements. Auditing standards classify assertions into five broad categories as follows:

- Existence or Occurrence
- Completeness
- Valuation or Measurement
- Rights and Obligations
- Presentation and Disclosure

b. Control Objectives (Control Categories)

Lookup Type: AMW CONTROL OBJECTIVES

Accessibility Level: Extensible

Control objectives provide a platform to help the auditor accomplish the following tasks:

- Accumulate sufficient competent evidence as required by audit standards.
- Decide on the proper evidence to accumulate given the circumstances of the audit engagement.

Control objectives can also be used to verify a control's design and operational effectiveness. Seeded values for control objectives are:

- Effectiveness and efficiency of operations
- Reliability of Financial Statements
- Compliance with applicable laws and regulations
- Safeguarding Information and Systems

Control Location

Lookup Type: AMW CONTROL LOCATION

Accessibility Level: Extensible

The control location refers to the geographic scope and implementation of the control. Seeded values for control locations are:

- Global
- Local
- Regional

Control Approval Status

Lookup Type: AMW CONTROL APPROVAL STATUS

Accessibility Level: System

The Approval Status of the Control. To be available for use in Oracle Internal Controls Manager, a Control must have a status of "Approved." Seeded values for control approval status are:

- Approved
- Draft
- Pending Approval
- Rejected

Controls Search

You can optionally search for a subset of controls using the following dimensions:

- Control Name
- Control Location
- Control Type
- Automation Type

Note: For more information, refer to the section Control Attributes., page 4-11

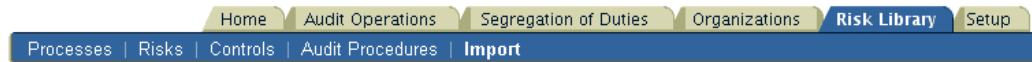
Importing Risks and Controls into Oracle Internal Controls Manager

As in the case of processes, companies build up libraries of risks and controls that apply to their organizations based on the nature of their businesses. With the import functionality in Oracle Internal Controls Manager, audit professionals can import risks and controls from a file thereby leveraging the presence of existing repositories.

Oracle Internal Controls Manager uses Oracle Web ADI for the import of risks, controls and risk-control associations. Web ADI provides many advantages including the use of a native spreadsheet interface. You can copy risk library objects into a spreadsheet and make use of the Web ADI framework to import them. The spreadsheet has a dynamic layout based on the risk objects being imported.

Use the Risk Library > Import tab in Oracle Internal Controls Manager to import risk and control objects into both the Risk library and organizations. Note that risks and controls constitute relatively static data and most organizations will therefore import this information infrequently.

| Topic | Navigation Path |
|---------------------------|--|
| Import Risks and Controls | Using a super user (or equivalent) responsibility, click the Risk Library tab and then the Import subtab |



[Import Processes](#)

[Import Risks and Controls](#)

[Import Risks and Controls in Organization](#)

[Import Controls](#)

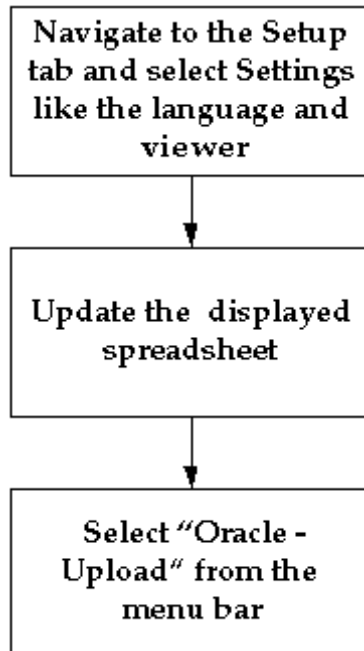
[Import Audit Procedures](#)

[Import Process to Key Account Associations](#)

Oracle Internal Controls Manager provides three paths for the import of risk and control objects:

- Import Risks and Controls (into the Risk Library)
- Import Risks and Controls in Organizations
- Import Controls

Note: While all risk and most control attributes can be imported using the import paths "Import Risks and Controls" and "Imports Risks and Controls in Organizations," the "Import Controls" path enables the detailed and complete import of control objects only.



As shown in the above diagram, Oracle Internal Controls Manager first requires that you select user settings like the language and viewer (Excel 1997/2000). The spreadsheet is then displayed and you can enter/copy values into these cells. Finally select Oracle - Upload from the menu bar to begin the import process.

Note: Web ADI is certified against Excel 2002 (XP). For more details, refer to Using Web ADI with Excel 2002 (XP), page 4-28

Import Risks and Controls (into the Risk Library)

Using the "Import Risks and Controls" hyperlink, audit professionals can import risks, controls, and their associations with processes into the Risk Library.

During the import, risks and controls are created if they do not exist and updated if they are already in the system. Attributes of risks and controls are the major part of the risk-control spreadsheet and objects are updated with these attributes.

The import also allows you to associate risks and controls with processes. Note that though the import of risks and controls can be done separately in this spreadsheet, the risk-control association does not exist by itself in the application i.e. risk and control objects can only be linked to one another in the context of a process. Hence your associated processes must reside in the Risk Library if you choose to link risks and controls with processes in the import.

Validation of the import data is done within the spreadsheet itself through lists of values for all lookup based columns.

The following table lists the fields in the import spreadsheet:

| Field Name | Mandatory | Validation |
|--------------|-----------|---------------------------------------|
| Process Code | No | All valid process codes in the system |
| Process Name | No | All valid processes in the system |

| Field Name | Mandatory | Validation |
|----------------------------------|--|---|
| Process Objective Name | No | Valid process objective names for objectives already stored in the system OR Enter the name for new process objectives. |
| Process Objective Description | No | None |
| Risk Name | Yes | Valid names for risks already stored in the system OR Enter the name for new risks. |
| Revise Risk | No | Y/N |
| Risk Description | Yes | None |
| Compliance (Risk Type) | At least one of the four risk types is mandatory | Y/N |
| Efficiency (Risk Type) | At least one of the four risk types is mandatory | Y/N |
| Financial Statements (Risk Type) | At least one of the four risk types is mandatory | Y/N |
| Misconduct (Risk Type) | At least one of the four risk types is mandatory | Y/N |
| Likelihood | Yes | AMW_LIKELIHOOD |
| Impact | Yes | AMW_IMPACT |
| Material Risk | No | Y/N |
| Material Value | No | None |
| Risk Approval Status | No | Approved, Draft |
| Risk Classification | No | All valid Risk Classifications in the system |
| Control Name | No | Valid names for controls already stored in the system OR Enter the name for new controls |
| Revise Control | No | Y/N |
| Control Description | No | None |
| Associate Audit Procedure | No | Valid names of audit procedures already stored in the system |

| Field Name | Mandatory | Validation |
|--------------------------|-----------|--|
| Design Effectiveness | No | Y/N |
| Operating Effectiveness | No | Y/N |
| Control Approval Status | No | Approved, Draft |
| Control Location | No | AMW_CONTROL_LOCATION |
| Control Type | No | AMW_CONTROL_TYPE |
| Automation Type | No | AMW_AUTOMATION_TYPE |
| Application | No | To restrict the values in the Controls Source list of values. Refer to Automation Type in the section on Control Attributes, page 4-11 |
| Control Source | No | Valid Control Sources. Refer to Automation Type in the section on Control Attributes, page 4-11 |
| Physical Evidence | No | None |
| Business Group | No | PER_BUSINESS_GROUPS table. Accessible under Work Structures -> Organizations in Oracle Human Resources. The Business Group is used to identify the job titles to be shown. If you have a (manual) control that needs to be signed, you can identify that individual's minimum level using the job title. The Business Group is typically obtained from the user profile when the user is logged into the application. However, the same is not available from a WebAdi session and hence the need to enter this info during control upload. |
| Job Name | No | PER_JOBS table. Accessible under Work Structures -> Jobs in Oracle Human Resources. The Business Group column must be populated to see the associated Job Name. |
| Preventive Control | No | Y/N |
| Detective Control | No | Y/N |
| Disclosure Control | No | Y/N |
| Key Control | No | Y/N |
| Verification Source | No | Form, Report |
| Verification Source Name | No | None |
| Verification Instruction | No | None |
| Control Classification | No | All valid control classifications in the system |

| Field Name | Mandatory | Validation |
|---|-----------|------------|
| Ctrl Comps (Control Components) - Control Activities | No | Y/N |
| Ctrl Comps (Control Components) - Internal Environment | No | Y/N |
| Ctrl Comps (Control Components) - Information and Communication | No | Y/N |
| Ctrl Comps (Control Components) - Monitoring | No | Y/N |
| Ctrl Comps (Control Components) - Risk Assessment | No | Y/N |
| Ctrl Comps (Control Components) - Objective Setting | No | Y/N |
| Ctrl Comps (Control Components) - Risk Response | No | Y/N |
| Ctrl Comps (Control Components) - Event Identification | No | Y/N |
| Ctrl Ctgrs (Control Categories) - Effectiveness and efficiency of operations | No | Y/N |
| Ctrl Ctgrs (Control Categories) - Reliability of Financial Statements | No | Y/N |

| Field Name | Mandatory | Validation |
|---|-----------|------------------------|
| Ctrl Ctgrs (Control Categories) - Compliance with applicable laws and regulations | No | Y/N |
| Ctrl Ctgrs (Control Categories) - Safeguarding Information and Systems | No | Y/N |
| User defined Control Categories 1 ... N | No | AMW_CONTROL_OBJECTIVES |
| Ctrl Asserts (Controls Assertions) - Existence or Occurrence | No | Y/N |
| Ctrl Asserts (Controls Assertions) - Completeness | No | Y/N |
| Ctrl Asserts (Controls Assertions) - Valuation or Measurement | No | Y/N |
| Ctrl Asserts (Controls Assertions) - Rights and Obligations | No | Y/N |
| Ctrl Asserts (Controls Assertions) - Presentation and Disclosure | No | Y/N |
| User defined control assertions 1 ... N | No | AMW_CONTROL_ASSERTIONS |

Import Risks and Controls in Organizations

Using the "Import Risks and Controls in Organizations" hyperlink, audit professionals can import risks, controls, and their associations with specific organizational processes in the application.

Note that applicable organizational processes must reside in the application before you can execute this import. Hence the prerequisites for the import are:

1. Setup valid organizations in the application

2. Import processes into the Risk Library and associate these processes to the organizations

The new risk and control objects are imported into BOTH the Risk Library and applicable organizations. Validation of the import data is done within the spreadsheet itself through lists of values for all lookup based columns. During the import, risks and controls are created if they do not exist and updated if they are already in the system. Attributes of risks and controls are the major part of the risk-control spreadsheet and objects are updated with these attributes.

The fields in this import spreadsheet are exactly the same as those listed in the previous section (for the Import of Risks and Controls into the Risk Library) with the following two exceptions:

- The mandatory Organization Name at the top of the spreadsheet. Note that you can import the data into only one organization at a time.
- Process Names are mandatory as well. This import is for the creation of risk and control objects and their association with specific organizational processes.

Note the following points with regard to the import of risks and controls in both Risk Library and organizations:

1. For user defined control categories (control objectives) and control assertion columns to appear in the spreadsheet, they must first be defined in the Oracle Internal Controls Manager Lookup Tables (under the AMW_CONTROL_OBJECTIVE and AMW_CONTROL_ASSERTIONS Lookup Types). It is **mandatory** that these lookups also have an associated Tag Number when set up. Using the Internal Controls Manager Super User (Forms) or equivalent responsibility, navigate to the Lookup windows to complete this task.
2. Web ADI uploads the data from the spreadsheet into the AMW_RISKS_CONTROLS_INTF interface table. A concurrent program then uploads the data from the interface table to the base tables. Any errors that occur during the import process are flagged as errors with appropriate error messages.
3. You may import and link (with processes) risks and controls that have a status of "Draft." However when a process is submitted for approval, the application will validate that all associated risk and control objects are first approved. If not, the submission for process approval will be rejected.
4. The revise flag set to "Y" for either risk or control fields implies that the attributes of the risk and/or control will be updated with the values listed in the spreadsheet. Oracle Internal Controls Manager will then attach the new attribute values to the risk and control even if they are blank. The revise flag value "N" for either of these fields will indicate that the associated attribute values in the spreadsheet are to be ignored.
5. As noted earlier, all risk and most control attributes can be imported using the import paths "Import Risks and Controls" and "Imports Risks and Controls in Organizations." Use the "Import Controls" path for the detailed and complete import of control objects.
6. If set to "Yes," the profile option AMW: Risks Controls in Organization - Delete after Import will delete controls from the interface table after their successful import via WEBADI.

Import Controls

Using the "Import Controls" hyperlink, you can import the details of controls objects into the application.

The following table lists the fields in the import spreadsheet:

| Field Name | Mandatory Validation | |
|-------------------------|----------------------|--|
| Control Name | Yes | Valid control names for controls already stored in the system. For existing controls, the upload will update their attributes. You can enter the control name if it does not exist in the application. |
| Revise Control | No | Y/N |
| Control Description | Yes | None |
| Control Approval Status | No | Approved, Draft |
| Control Location | No | AMW_CONTROL_LOCATION |
| Control Type | Yes | AMW_CONTROL_TYPE |
| Automation Type | No | AMW_AUTOMATION_TYPE |
| Application | No | To restrict the values in the Controls Source list of values. Refer to Automation Type in the section on Control Attributes, page 4-11 |
| Control Source | No | Valid Control Sources. Refer to Automation Type in the section on Control Attributes, page 4-11 |
| Physical Evidence | No | None |
| Business Group | No | PER_BUSINESS_GROUPS table. Accessible under Work Structures -> Organizations in Oracle Human Resources. The Business Group is used to identify the job titles to be shown. If you have a (manual) control that needs to be signed, you can identify that individual's minimum level using the job title. The Business Group is typically obtained from the user profile when the user is logged into the application. However, the same is not available from a WebAdi session and hence the need to enter this info during control upload. |
| Job Name | No | PER_JOBS table. Accessible under Work Structures -> Jobs in Oracle Human Resources. The Business Group column must be populated to see the associated Job Name. |
| Preventive Control | No | Y/N |
| Detective Control | No | Y/N |
| Disclosure Control | No | Y/N |
| Key Control | No | Y/N |

| Field Name | Mandatory Validation | |
|--|----------------------|---|
| Verification Source | No | Form, Report |
| Verification Source Name | No | None |
| Verification Instruction | No | None |
| Unit of Measure | No | Per the profile option AMW: Unit of Measure Class for Control Frequency |
| Control Frequency | No | NA |
| Control Classification | No | All valid Control Classifications in the system |
| Ctrl Comps (Control Components) - Control Activities | No | Y/N |
| Ctrl Comps (Control Components) - Internal Environment | No | Y/N |
| Ctrl Comps (Control Components) - Information and Communication | No | Y/N |
| Ctrl Comps (Control Components) - Monitoring | No | Y/N |
| Ctrl Comps (Control Components) - Risk Assessment | No | Y/N |
| Ctrl Comps (Control Components) - Objective Setting | No | Y/N |
| Ctrl Comps (Control Components) - Risk Response | No | Y/N |

| Field Name | Mandatory Validation | |
|--|----------------------|-----|
| Ctrl Comps (Control Components) - Event Identification | No | Y/N |
| Ctrl Ctgrs - Effectiveness and efficiency of operations | No | Y/N |
| Ctrl Ctgrs - Reliability of Financial Statements | No | Y/N |
| Ctrl Ctgrs - Compliance with applicable laws and regulations | No | Y/N |
| Ctrl Ctgrs - Safeguarding Information and Systems | No | Y/N |
| Ctrl Asserts - Existence or Occurrence | No | Y/N |
| Ctrl Asserts - Completeness | No | Y/N |
| Ctrl Asserts - Valuation or Measurement | No | Y/N |
| Ctrl Asserts - Rights and Obligations | No | Y/N |
| Ctrl Asserts - Presentation and Disclosure | No | Y/N |
| Ctrl Purposes - Initiating | No | Y/N |
| Ctrl Purposes - Processing | No | Y/N |

| Field Name | Mandatory Validation | |
|---------------------------|----------------------|-----|
| Ctrl Purposes - Recording | No | Y/N |
| Ctrl Purposes - Reporting | No | Y/N |

If set to "Yes," the profile option AMW: Controls - Delete after Import will delete controls from the interface table after their successful import via WEBADI.

Using Web ADI with Excel 2002 (XP)

For Web ADI to work with Excel 2002 (XP), perform the following three steps:

1. Open Excel 2002
2. Go to Tools -> Macro -> Security -> Trusted Sources
3. Check the "Trust access to Visual Basic Project"

Note: For more information, refer to Importing Processes using Web ADI, page 2-12

Export Risk and Control Objects

The application allows you to export Risk Library objects and associations from the database using Web ADI. Use this **DOWNLOAD** feature to compare and synchronize the database information with any spreadsheets that you maintain outside Oracle Internal Controls Manager. The format of the download spreadsheets mirror those used for the corresponding upload.

Export Risks and Controls

| Topic | Navigation Path |
|-----------------------------|--|
| Download Risks and Controls | Using a super user (or equivalent) responsibility, click the Risk Library tab and then the Processes subtab. Drill down into the appropriate Process to access the Download RCM button. |

Export Controls

| Topic | Navigation Path |
|-------------------|--|
| Download Controls | Using a super user (or equivalent) responsibility, click the Risk Library tab and then the Controls subtab to access the Download Controls button. |

Audit Procedures in Internal Controls Manager

This chapter covers the following topics:

- Introduction
- Setting up Audit Procedures in Oracle Internal Controls Manager
- Importing Audit Procedures into Oracle Internal Controls Manager
- Creating Audit Procedures within an Audit Engagement

Introduction

Auditors need to acquire an understanding of the internal control structure to assess control risk. This assessment is made in relation to control assertions and objectives in the organization's control environment.

Note: For more information, refer to Control Assertions and Objectives in the section Control Attributes, page 4-11.

Whether control policies, systems, and measures are believed to be effectively designed or not, auditors will assess the risk to be at a level that reflects their evaluation of an organization's internal controls. In all cases, once a control risk assessment is made, audit procedures must be designed to test the controls.

Audit procedures provide detailed steps to be performed during audit fieldwork. They are designed to achieve specific audit objectives by validating the effectiveness of controls, in terms of their design as well as their operation. Audit procedures in Oracle Internal Controls Manager can therefore be identified as verifying design effectiveness, operating effectiveness, or both.

Audit procedures to test the effectiveness of controls involve activities like the following:

- Inquiries of client personnel
- Examination of documents and records
- Accounting for the integrity of transactions. For example, this can take the form of checking the numerical sequence of invoices.
- Observation of the application of policies and procedures

In Oracle Internal Controls Manager, you can associate audit procedures with the controls that the procedures are supposed to verify. You can also verify the details of all the past results for each audit procedure.

Setting up Audit Procedures in Oracle Internal Controls Manager

Audit procedures provide detailed steps to be performed during audit fieldwork. The following measures must be undertaken to set up and use audit procedures in Oracle Internal Controls Manager:

- 1. Create audit procedures
- 2. Associate audit procedures with controls.
- 3. Enter testing results for audit procedures in Audit Engagements

Note: Instead of creating audit procedures manually and then associating them with process controls, Oracle Internal Controls Manager provides a powerful import mechanism for audit procedure objects.

Using this import functionality you can import audit procedures and associate them with controls in a single step. For more information, refer to the section Importing Audit Procedures into Oracle Internal Controls Manager, page 5-5.

You can view all created audit procedures in the main Audit Procedures window by navigating to the Risk Library > Audit Procedures sub-tab.

1. Create Audit Procedures

| Topic | Navigation Path |
|-------------------------|--|
| Create Audit Procedures | Using an Oracle Internal Controls Manager Super User (or equivalent) responsibility, navigate to the Risk Library tab and the Audit Procedures sub tab to access the Create button. The procedure is created for a particular classification. |

Note: For more information on Classifications, refer to Extensible Attributes in Oracle Internal Controls Manager, page 14-1.

The screenshot shows the 'Create Audit Procedure' window. At the top, there are tabs: Name, Description, End Date, Class, and Financial Audit Procedure. The 'Name' tab is selected. Below the tabs, there is a 'Name' text field and a 'Description' text area. To the right of the 'Name' field are buttons: 'Cancel', 'Save for later', and 'Submit'. Below the 'Description' area is a 'File Date' field with a calendar icon. Below the 'File Date' field is a 'Class' field with a dropdown arrow. Below the 'Class' field is a 'Financial Audit Procedure' field with a dropdown arrow. At the bottom of the window, there is a table with the following columns: 'Selected Name', 'Description', 'Design Effectiveness', and 'Operating Effectiveness'. The table contains one row with the value 'Risk Library'.

In the Create Audit Procedure window you can choose to End Date the procedure.

If you save the procedure for later editing, the procedure is created with a status of "Draft." When the procedure is finalized, click on Update in the main Audit Procedures page and then submit the procedure for approval. If you need to update an approved procedure, drill into the procedure details and then select Update.

Note that risk library objects can only be utilized in the application after they are approved. Audit procedures are approved/reapproved based on your setup of workflow rules and the approval hierarchy in the Oracle Approvals Management application. When the approval is complete, the procedure approval status changes to Approved.

Note: The approval process for approving risk library objects is optional. For more details, refer to Manage the Process Risk Library, page 6-1.

Audit Procedure Steps: When seeding audit procedures in Oracle Internal Controls Manager, you can also create its steps by entering the details of tasks that make up the procedure. Audit Steps allow the assignment of work at the most granular level needed to accomplish the audit task.

| Topic | Navigation Path |
|------------------------------|--|
| Create Audit Procedure Steps | Drill into an existing audit procedure to access the Steps subtab. |

Enter a sequence number for a chronological listing of the step. You can optionally enter a sample size for the data to be worked on in a particular step.

2. Associate Audit Procedures with Controls

| Topic | Navigation Path |
|--|---|
| Associate Audit Procedures with Controls | Drill into an existing audit procedure to access the Controls subtab. |

Home | Audit Operations | Segregation of Duties | Organizations | Risk Library | Setup

Processed | Risks | Controls | Audit Procedures | Significant Accounts | Monitor

Review Audit Procedures | Select Classification |

Create Audit Procedure

Includes required fields

Name: Review A/R trial balance for unusual receivables

Description:

End Date:

Internal Audit Procedure

Controls | Attachments | Files | Sub-Process Tasks | Manual Sub-Procedure

Select Control Associations to: Remove | Add Controls

Select All | Select None

| Select Name | Description | Design Effectiveness | Operating Effectiveness |
|---|---|----------------------|-------------------------|
| <input type="checkbox"/> Sales Manager Approves | Sales Manager Approves | Yes | Yes |
| <input type="checkbox"/> Pricing Policy | Price reduction applied to all products from the public | Yes | No |

Audit procedures are written to verify the effectiveness of the organization's internal controls. Once audit procedures are created, the next step is to associate them with controls that you have set up in the system.

The Controls subtab shows all controls that this procedure is related with and you can search for additional controls to link with the audit procedure. When you associate a control with an audit procedure in Oracle Internal Controls Manager, you can identify if it is intended to verify design effectiveness, operating effectiveness or both.

3. Enter Results for an Audit Procedure in an Audit Engagement

| Topic | Navigation Path |
|--|---|
| Enter results and opinions for an audit procedure | <p>Using an Internal Auditor (or equivalent) responsibility, navigate to the Audit Operations tab. Click on Engagement subtab and drill into the details of the appropriate engagement.</p> <p>Select the Task faint tab and drill into the task to access the audit procedure linked to that task. Then click on the Status column hyperlink for this audit procedure to update the procedure with a result.</p> |
| Enter control evaluation based on an audit procedure | <p>Using an Internal Auditor (or equivalent) responsibility, navigate to the Audit Operations tab. Click on Engagement subtab and drill into the details of the appropriate engagement.</p> <p>Click on Control faint tab at the engagement detail page and then on the Show hyperlink (for a control) to show audit procedures for the control. Click on the Evaluate Control icon to enter the control evaluation based on this particular audit procedure.</p> |

Note: For details on entering results and evaluations for procedures in an engagement, refer to Audit Engagements in Oracle Internal Controls Manager, page 8-1.

You can at any time, drill into the Audit Procedure Details to view the controls that the audit procedure is verifying.

It is important to note that a business process that is executed in a particular environment will incur a unique risk. The same process running in a different environment can result in a different level of risk. Audit results and opinions are therefore entered for controls mitigating process risk within specific organizations.

Importing Audit Procedures into Oracle Internal Controls Manager

As with processes and other risk library objects, companies build up libraries of audit procedures that apply to their organizations based on the nature of their businesses. With the import functionality in Oracle Internal Controls Manager, audit professionals can import audit procedures from a file thereby leveraging the presence of existing repositories.

Oracle Internal Controls Manager uses Oracle Web ADI for the import of audit procedures and procedure-control associations. Use the Risk Library tab in Oracle Internal Controls Manager to import audit procedures.

| Topic | Navigation Path |
|-------------------------|--|
| Import Audit Procedures | Using a super user (or equivalent) responsibility, click the Risk Library tab and then the Import subtab to access the option "Import Audit Procedures." |

To Import Audit Procedures

Use the "Import Audit Procedures" hyperlink to import procedures and associate them with controls in the application.

Note: You cannot create control objects during this import. All controls must be created before you can link them with audit procedures in the spreadsheet.

Note: Note that it is not mandatory to associate controls with audit procedures during the import.

During the import audit procedures are created if they do not exist and updated if they are already in the system. Attributes of the audit procedures are the major part of the spreadsheet and objects are updated with these attributes. Validation of the import data is done within the spreadsheet itself through lists of values for all lookup based columns.

The following table lists the fields in the import spreadsheet:

| Field Name | Mandatory | Validation |
|--------------------------------|-----------|--|
| Audit Procedure Name | Yes | None |
| Description | No | None |
| Approval Status | No | Draft, Approved |
| End Date | No | (MM-DD-YYYY) |
| Revise | No | (Y/N) |
| Control Name | No | Valid names for controls already stored in the application |
| Design Effectiveness | No | (Y/N) |
| Operating Effectiveness | No | (Y/N) |
| Step Number | Yes | None |
| Step Name | Yes | None |
| Step Description | No | None |
| Sample Size | No | None |
| Audit Procedure Classification | No | All valid classifications for audit procedures |

Web ADI uploads the data from the spreadsheet into an interface table. A concurrent program then uploads the data from the interface table to the base tables. Any errors that occur during the import process are flagged as errors with appropriate error messages.

Creating Audit Procedures within an Audit Engagement

In addition to the usual method of creating or importing Audit Procedures in the Risk Library, you can also create Audit Procedures within the course of an Audit Engagement. The requirement for running these procedures will normally arise during the course of the engagement.

Note: For more information, refer to Creating Audit Procedures within the scope of an Audit Engagement, page 5-6.

Risk Library Change Control

This chapter covers the following topics:

- Introduction
- Manage the Risk Library

Introduction

Regulations in many countries impose a burden on management for establishing and maintaining an adequate internal control structure in an enterprise. Annual reports must often contain an assessment of the effectiveness of the internal control structure and procedures for financial reporting. In addition, external auditors are often required to express an opinion on management's assertion of the adequacy of internal controls.

There are two important tasks that must be undertaken to establish the adequacy of an enterprise's internal control structure:

1. Identify, approve, and certify the business processes of the enterprise.

Note: For detailed information on defining and approving processes in Oracle Internal Controls Manager, refer to Overview of Process Setups in Oracle Internal Controls Manager, page 2-1 and Process Approvals and Change Management, page 3-1.

2. Manage all other objects in the risk library as described in this chapter. These are the risks, controls, and audit procedures related to the firm's business processes.

Manage the Risk Library

Note: As noted above, this chapter applies to risk, controls, and audit procedure objects.

An important benefit of Oracle Internal Controls Manager is its ability to leverage the presence of libraries of reusable risk library objects that can be associated with the business process within an organization. However, a key success factor in the use of these libraries is the accuracy of their data.

To maintain the integrity of information within the risk library, creation or modification of library items in Oracle Internal Controls Manager is controlled by an approval process. Therefore, when any library object is created or modified, a new revision of the object is created with a status "Draft."

Draft library objects can be associated with processes and organizations, but no auditing can be performed on them. Before a process can be submitted for approval, all its associated library objects like risks, controls, etc. must first be approved. Only approved processes can be assigned to organizations and hence used in the application.

All requests for the creation or modification of risk library objects are submitted for approval to approvers defined in Oracle Approvals Management.

Note: The use of Oracle Approvals Management is optional. If you choose not to go through the approval process, the profile option AMW: Disable Workflow Approval must be set to "Yes." In this case, the risk library objects are automatically approved (clicking the Submit button has no effect).

The Oracle Approvals Management application provides the following features:

- The ability to route approvals based on a hierarchy. Hierarchies are defined using Approval Rules set up in Oracle Approvals Manager. You can define a different approval hierarchy for different types of items in the risk library.

Each type of item which goes through an approval process is defined as a "Transaction Type" in the Approval Manager. Transaction types are defined for risks, controls, and audit procedures.

- The ability to review and monitor the approval process (for example, through notifications or workflow process diagrams using the Workflow Monitor).

Oracle Approvals Management provides a generic workflow approval system as a default. If no specific approval rules are defined for an object, then a "Default Approver" will be notified.

Note: For more information on setting up approval rules for risks, controls, and audit procedures, refer to the *Oracle Approvals Management Implementation Guide*.

To use Oracle Approvals Management, you must set the following:

- The profile option AMW: Disable Workflow Approval must be set to "No."
- A Workflow Background Process having the Item Type AMW: Generic Approvals must be active.
- The profile option AMW: Time-out limit for Control, Risk and Audit Procedure Approval (number, in days) can be used to restrict the response time from Oracle Approvals Management.

Certifying New Objects in the Risk Library

When any of these risk library objects are created, the item's Approval Status is set to "Draft." Drill down into the object's details page and click Submit to initiate a workflow process and notify approvers based on rules defined in the Oracle Approvals Management module.

When all approvals are complete, the Approval Status changes to "Approved." In case the record is rejected, the status changes to "Rejected." Note that you can save a record in "Draft" Approval Status and update it at any time prior to submission.

The following table lists the details of Approval Statuses for risk library objects in Oracle Internal Controls Manager:

| Library Object | Seeded Values | Lookup Type | Accessibility Level |
|------------------|--|---------------------------------|---------------------|
| Risks | Approved Draft Pending Approval Rejected | AMW_RISK_AP PROVAL_STATUS | System |
| Controls | Approved Draft Pending Approval Rejected | AMW_CONTROL_AP PROVAL_STATUS | System |
| Audit Procedures | Approved Draft Pending Approval Rejected | AMW_PRCDR_AP PRV_STATUS | System |

Note: For information on creating new risk library objects, refer to the following sections:

- Setting up Risks in Oracle Internal Controls Manager, page 4-2.
- Setting up Controls in Oracle Internal Controls Manager, page 4-10.
- Setting up Audit Procedures in Oracle Internal Controls Manager, page 5-2.

Revising Objects in the Risk Library

After a library item is approved, you cannot modify the current approved version of that item. Instead Oracle Internal Controls Manager allows you to create a new version and submit it for approval. Note that this submission triggers another workflow approval process.

Create a new revision of a Risk, Control, or Audit Procedure by navigating to the details section of the object from the home page or search results page and clicking the Update button. This revision is then submitted for approval. Once the new version of the item is approved, the newly created object becomes the latest approved copy and the old "Approved" object is available under the "History" section in the item's detail page.

If a revision already exists and is pending "Approval," then you can modify the details of that revision as long as the changes are not submitted for approval. Any changes will be saved under the current revision. A new revisions will also be generated if the old record had a "Rejected" status.

The following table lists the details of Revision statuses for risk library objects in Oracle Internal Controls Manager:

| Library Object | Seeded Values | Lookup Type | Accessibility Level |
|-----------------------------------|--|------------------------------|---------------------|
| Risks, Controls, Audit Procedures | Inactive Revised Objects Unapproved New Revision Approved | AMW_REVISION_V IEW_CHOICE | System |

Approval and Revision Status Values

The (Approval) Status and Revision states of a risk library object provide important information regarding its authority and certification. For a risk library object to be used in an audit engagement, it must be "Approved."

| Risk Name | Revision Number | Approval Status | Risk Likelihood | Risk Impact | Mitigation | Revision Status | Update Delete |
|---------------------------|-----------------|-----------------|-----------------|---------------|------------|-----------------|---------------|
| Duplicate Payments | 1 | Approved | Common | Major | Yes | Approved | |
| Fraud and Revenue | 1 | Approved | Unlikely | Medium | Yes | Approved | |
| Vendor Price List | 1 | Approved | Rare | Major | Yes | Approved | |
| Inventory Management | 1 | Approved | Rare | Insignificant | Yes | Approved | |
| Calculate Vendor Payments | 2 | Draft | Common | Minor | | New Revision | |
| Credit Pricing | 1 | Approved | Rare | Insignificant | Yes | Approved | |
| Unauthorized Payments | 1 | Approved | Medium | Major | No | Approved | |
| Accounts Receivable | 1 | Approved | Medium | Major | No | Approved | |

Initial Creation of a Risk Library Object

When you create an object, its Approval Status is "Draft" and the Revision Status is "Unapproved." When you submit the object for approval, the Approval Status becomes "Pending Approval" (Revision Status remains "Unapproved") and then "Approved" or "Rejected." The Revision Status changes to "Approved" only upon approval of the object.

Revision of a Risk Library Object

If you choose to Revise an Approved object, a new version is created with an Approval Status of "Draft" and a Revision Status of "New Revision." The Revision Status of the existing approved object becomes "Revised Object."

This revised version object can then be submitted for approval. Once approved both Approval Status and Revision status become "Approved." The Revision Status of the old Approved object becomes Inactive.

The following tables summarize the Approval and Revision Statuses of risk library objects.

Initial Creation of a Risk Library Object

| Action/State of the Risk Library Object | Approval Status | Revision Status |
|---|------------------|-----------------|
| Create a Risk Library object | Draft | Unapproved |
| Submit for approval | Pending Approval | Unapproved |
| On approval of the object | Approved | Approved |
| On rejection of the object | Rejected | Unapproved |

Revision of a Risk Library Object

| Action/State of the Risk Library Object | Revision | Approval Status | Revision Status |
|---|------------------|------------------|-----------------|
| Revise an approved object | Original Version | Approved | Revised Object |
| Revise an approved object | New Version | Draft | New Revision |
| Submit for approval | Original Version | Approved | Revised Object |
| Submit for approval | New Version | Pending Approval | New Revision |
| On approval of the revised object | Original Version | Approved | Inactive |
| On approval of the revised object | New Version | Approved | Approved |
| On rejection of the revised object | Original Version | Approved | Inactive |
| On rejection of the revised object | New Version | Rejected | New Revision |

Change History

Once the new version of the risk library object is approved, a copy of the old "Approved" object is stored and maintained for a historical record.

Every change that an item in the library has gone through is maintained as a part of the Risk, Control, or Audit Procedure history. You can view the history section from the details page of any risk library object in the Oracle Internal Controls Manager application.

Deletion of Approved Objects

| Topic | Navigation Path |
|---|---|
| Delete approved risks, controls, and audit procedures | Using the Oracle Internal Controls Manager Super User Forms (or equivalent) responsibility, run the concurrent request "Delete Objects." You may delete upto four objects at a time. |

Oracle Internal Controls Manager performs all necessary validations while running this process. You cannot delete objects that are associated with other approved risk library objects.

Assessments in Oracle Internal Controls Manager

This chapter covers the following topics:

- Introduction
- Integration with Oracle Scripting
- Creating an Assessment in Oracle Internal Controls Manager

Introduction

Oracle Internal Controls Manager gives you the ability to organize, document, and test internal controls and monitor ongoing compliance. You can use the application to conduct audit activities like the following:

- Define business processes and map them to an organization structure
- Record risks and controls and associate them with business processes
- Create audit procedures to test controls

With respect to testing controls as well as other tests like tests of details of balances, the amount of procedural work performed in an audit depends to a large extent on an auditor's assessment of the organization's internal control structure and compliance with established controls and regulations.

Oracle Internal Controls Manager therefore allows you to incorporate an assessment of the organization regarding its internal control structure and compliance. The assessment is made with respect to:

- Predefined components affecting the organization's audit environment. The seeded components shown below are from the COSO framework. You can also add your own values to this list:
 - The control environment
 - Risk Assessment
 - Control activities
 - Information and communication
 - Monitoring activities
 - Event Identification
 - Objective Setting

- Risk Response
- A particular organizational context. You can specify the context in terms of:
 - The organization itself
 - Controls in the organization
 - Business processes in the organization

An audit assessment requires auditors to have executed a systematic examination of the organization's information system that includes:

- Identifying security deficiencies and the adequacy of internal controls
- Sourcing the data from which to predict the effectiveness of controls
- Confirming the adequacy of the internal controls structure after implementation.

Once assessments are made and subsequent audit work performed, you can review the compliance of your business processes and systems and then issue audit reports and opinions.

Integration with Oracle Scripting

To help in making assessments, you can associate a survey written with the Oracle Scripting tool to an Assessment in Oracle Internal Controls Manager. Oracle Scripting is a powerful web based tool for soliciting, managing, and analyzing stakeholder feedback through surveys. In any organization, surveys created with Oracle Scripting can help in providing an effective control environment and the results can be used to make macro level risk assessments.

Oracle Scripting is comprised of several components including a Script Author and a Survey Administration console. The Script Author is used to build "survey scripts" that can be deployed throughout the enterprise. With the Survey Administration console, you can establish and maintain survey campaign information as well as generate reports for analyzing survey data.

There are various ways in which scripts can be employed to gather data. For example, a script can serve as a survey questionnaire to solicit specific information from employees or any other target population. A script can also be written to integrate different aspects of multiple applications together.

For any survey, the Scripting tool provides the following capabilities:

- Ability to ask different questions based on responses. For example, if the respondent's answer to a series of questions indicates a high risk in some area, the survey can "drill down" into the specifics of the problem, leading to the collection of more detailed information for the assessor.
- Ability to ask different sets of questions for different target respondents or lines of business.
- Ability to set "triggers" within a survey to alert assessors of specific results.

Once a script is created, it can then be used as part of a survey campaign. The application can be used to identify survey participants, deploy the survey via e-mail, and allow respondents to fill out questionnaires via the internet. Survey campaigns can be targeted to cover specific lines of business as well as specific groups. You can then use the survey results to provide data on common themes or risk areas.

Using these features, an audit related survey can provide valuable insight into the functioning of the organization, process, or control/control structure. Since Oracle Internal Controls Manager allows you to associate a survey to an Assessment, the survey results provide credibility and support to your Assessment.

Survey Creation Process

The major steps to create and manage surveys are listed below:

1. Author the survey questionnaire using the Script Author
2. Define a Survey Campaign via the Survey Administration utility
3. Deploy the survey using the Survey Administration Console
4. Monitor and analyze responses

Note: For more information on the survey creation process, survey administration, and survey reporting, refer to the *Oracle Scripting Implementation Guide* and the *Oracle Scripting Developer's Guide*.

Confidential Feedback Mechanism

Oracle Scripting also enables you to effectively monitor operations by providing a confidential feedback mechanism. This is a mandatory feature in certain geographic regions.

For example, the Sarbanes Oxley Act in the USA requires the audit committee of a public company to establish procedures for the receipt of confidential and anonymous submissions from employees regarding questionable accounting or auditing matters. This "whistle-blower" provision now requires employers to provide all employees with a safe way to deliver anonymous feedback.

Using Oracle Scripting, you can create and deploy surveys where employee confidentiality is maintained. Scripts can be written to capture information from employee hotline calls and multiple anonymous calls from the same person can be linked.

Survey Reporting

Survey results are available immediately via out of the box Discoverer reports. The reports are available from Oracle Business Intelligence and you can modify the Discoverer workbooks to create ad hoc reports. You can use Discoverer to export all your report data to external systems, such as to an Excel spreadsheet.

Note: For more information on reports available via Interaction Center Intelligence, refer to the *Oracle Scripting Implementation Guide*.

Some of the seeded reports are listed below:

Survey Question Frequency Report: This report can be used to show how people have responded to survey questions at a summary level for each survey deployment. It shows the frequency of response for any question that is a non-text question. For example, how many people responded yes, how many responded no to the question "Are you satisfied with your audit?"

Survey Question Detail Report: Provides all of the respondent's answers to each question for all people who have responded to the survey.

Survey Deployment Text Responses Report: Extracts just the text responses so that managers can review the information in detail. Text responses often hold comments and other critical free form information. This report is useful for supervisors or managers who want to get an overall flavor for the comments that individual respondents have provided within the survey.

Survey Campaign Summary Report: This report provides summary information on each survey campaign. It shows at a glance how many surveys have been sent out, the response ratio, the number of errors (for example bad e-mail addresses), and how many surveys have been aborted (no questions answered).

Survey Deployment Detail Report: Shows detailed information about a deployment for each survey including the name of the list of target respondents, how many reminders have been sent out, response ratio, etc.

Creating an Assessment in Oracle Internal Controls Manager

Oracle Internal Controls Manager enables you to record your assessment of the organization's internal control structure and compliance with established controls and regulations. As mentioned earlier, the amount of procedural work performed in an audit depends to a large measure on this up front assessment.

You can record the essential attributes of the Assessment as well as evaluations of the assessment results. Oracle Internal Controls Manager provides optional integration with Oracle Scripting to associate a survey conducted with that application to the Oracle Internal Controls Manager Assessment.

To Create an Assessment

The steps to create an Assessment in Oracle Internal Controls Manager are listed below:

1. Enter the essential attributes of the Assessment
2. Record the context in which the Assessment is conducted
3. Optionally associate the Assessment to one or more surveys created using Oracle Scripting
4. Optionally create and set up Assessment Procedures
5. Record an audit opinion/evaluation of the Assessment

1. Enter the Essential Attributes of the Assessment

| Topic | Navigation Path |
|----------------------|---|
| Create an Assessment | Using the Internal Auditor (or equivalent) responsibility, navigate to the Audit Operations tab and then the Assessments subtab. Then click the Create button. |

As the first step, create the assessment by setting up attributes like its Owner Name and Expected Completion Date.

[Home](#)
[Audit Operations](#)
[Segregation of Duties](#)
[Organizations](#)
[Risk Library](#)
[Setup](#)

[Assessments](#)
[Engagements](#)
[Findings](#)
[Remediation](#)

Audit Operations: Assessments >

Create Assessment

* Indicates required field

[Cancel](#) [Apply](#)

Summary

* Name

Type

* Owner Name

Assessment Period

Expected Completion Date

(example: 21-Mar-2005)

Status

Description

Components

[Select All](#) | [Select None](#)

| Select Name |
|--|
| <input type="checkbox"/> Control Activities |
| <input type="checkbox"/> Internal Environment |
| <input type="checkbox"/> Event Identification |
| <input type="checkbox"/> Information and Communication |
| <input type="checkbox"/> Monitoring |
| <input type="checkbox"/> Objective Setting |
| <input type="checkbox"/> Risk Assessment |
| <input type="checkbox"/> Risk Response |

The following table provides further information on select fields in the Assessment page.

| Field | Details | Seeded Values | Lookup Type | Accessibility Level |
|-------------------|---|--|-----------------------|---------------------|
| Type | User defined Assessment classification | Compliance Assessment Control Environment Assessment Comprehensive Self Assessment Risk Assessment Security Assessment | AMW_ASSESSMENT_TYPE | User |
| Status | The status of the Assessment. Changing the status is a manual step. Once the assessment definition is complete and the assessment is started, the user can change the status from "Not Started" to "In Process." | Archived Completed Not Started In Process | AMW_ASSESSMENT_STATUS | System |
| Assessment Period | | | | |

Components

Your assessment regarding internal control structure and compliance is made with respect to certain "Components" that affect the organization's audit environment. When you create an Assessment, Oracle Internal Controls Manager allows you to specify these Components.

The seeded components shown below are from the COSO framework in the USA. You can also add your own values to the list.

The Control Environment: This is the control conscience of an organization, the "tone at the top." When making an assessment on the control environment, consider factors such as:

- The presence of a code of ethics as well as mandatory training on this code
- Documented policies and procedures
- Aggressiveness of profit plans and budget data

Risk Assessment: An evaluation of internal and external factors that impact an organization's performance. Consider the presence of formal program offices for the following:

- Business risk management
- Process risk management
- Internal audit risk assessment

Control Activities: The policies and procedures to help ensure that actions identified to manage risk are executed and timely. These policies generally fall into the six categories listed below:

- Segregation of duties
- Proper procedures for approvals and delegation of authority
- Adequate processes/systems to maintain records and an audit trail, independent checks on performance
- Physical control over assets and records
- Account reconciliations
- Information technology controls

Information and Communication: The process which ensures that relevant information is identified and communicated in a timely manner. When making an assessment on this component, consider the following:

- Messages from senior management regarding control
- Formal operating plans
- Employee job descriptions, policies covering employee behavior such as conflicts of interest
- Training on formal codes of conduct

Monitoring Activities: The process to determine whether the internal control is adequately designed, effectively executed, and adaptive. This assessment will depend to a large extent on whether an internal audit function is established within the organization to monitor the efficiency and effectiveness of other control related policies and procedures.

To minimize risk, it is essential that the internal audit staff be independent of both operating and accounting departments. They should also report directly to an audit committee.

Event Identification: An event is an occurrence that could affect achievement of objectives and can have positive or negative impact or both. Risks are the possibilities that these events will occur.

Objective Setting: Firms select objectives that support their strategy and mission and which align with their preferred risk appetite. The objectives reflect management's strategic choices as to how the entity will seek to create value for its stakeholders. It is therefore imperative that management also identifies the risks associated with these strategy choices and considers their implications.

Risk Response: This component involves the identification and evaluation of possible responses to Events.

Note: The check boxes displayed in the Components section come from the lookup AMW_ASSESSMENT_COMPONENTS. The lookup values can be changed as needed to provide additional Assessment components.

2. Record the Context in which the Assessment is Conducted

| Topic | Navigation Path |
|-------------------------|---|
| Record a Survey Context | Navigate to the Audit Operations > Assessments tab and select the Assessment for which you need to record a Context. Drill into the Contexts subtab and then click the Add button. |

To record a context for the Assessment, the status of the Assessment must be "Not Started." You cannot record a context if the Assessment has any other status.

Your assessment is made with reference to one of more of the following:

- A particular organization
- Processes within that organization
- Controls associated with those organizational processes (through the process-risk-control matrix)

Values in each page of the train are filtered by the selections made in earlier pages.

3. Associate the Assessment with surveys created using Oracle Scripting (Optional)

| Topic | Navigation Path |
|--|---|
| Associate an Assessment with one or more Surveys | <p>Navigate to the Audit Operations > Assessment tab and select the particular Assessment to be associated with a Survey.</p> <p>Click on the Survey subtab and then the Add button.</p> |

You can initiate a survey campaign to incorporate employee and stakeholder feedback on internal controls. The Add Survey to Assessment page shows the following fields:

The Survey: The survey campaign, at the highest level of the survey hierarchy, is where parameters affecting the entire survey campaign are administered. These parameters include the specific script to be used as the survey questionnaire, the survey status (open and cancelled), and survey resources. A survey campaign contains one or more cycles (described below).

The Survey Cycle: Allows you to differentiate different time frames for running the survey. Survey Cycle attributes include a minimum response percentage and status (open, active, or cancelled). The ability to define multiple cycles in a survey campaign aids in comparative data analysis for surveys to be conducted over a span of time. Each cycle contains one or more deployments (described below).

The Survey Deployment: A deployment belongs to a particular cycle and is the lowest member of the survey hierarchy. Essentially, deployments are the construct within the survey campaign that contains key business rules (the "who," "when," and "how long") for that portion of the survey campaign. A deployment must be made active before respondents can participate in a survey campaign.

Note: You can only link the Assessment in Oracle Internal Controls Manager to the survey name, cycle, and deployment.

Use the Oracle Scripting application to view the results of the survey. For more information, refer to the *Oracle Scripting Implementation Guide*.

You can only associate surveys that do not have the status (of the survey, survey cycle or deployment) "Closed" or "Cancelled." Also, the Response End Date of the deployment should be a future date.

Also, if the Assessment is "In Process" and has an "Active" survey associated with it, then you cannot update the survey parameters in the Add Survey to Assessment page.

Note: An "Active" survey is one which is deployed to participants and is in the process of being updated.

4. Optionally create and set up Assessment Procedures

| Topic | Navigation Path |
|------------------------------|--|
| Create Assessment Procedures | Navigate to the Audit Operations > Assessment tab and select the appropriate Assessment. Click on the Procedures subtab. Use the Add button to add a previously created procedure and the Create button to write up a new procedure that will be appended to this Assessment. |

Home Audit Operations Segregation of Duties Organizations Risk Library Setup

Assessments Engagements Findings Remediation

Audit Operations: Assessments > Assessment Details: Finance Process Assmt >

Create Assessment Procedure

* Indicates required field

* Name Review procedures for approvals Description

End Date (example: 22-Mar-2005)

Cancel Apply

Assessment Procedure Steps

| *Sequence | *Name | Description | Sample Size | Delete |
|-----------|--------------------|---------------------------|-------------|--------|
| 10 | Pre-requisite Step | Collect operating manuals | 20 | |
| 20 | Review | Review approval procedure | 20 | |
| 30 | Test | Create a dummy line of cr | 3 | |

Add Another Row

You can associate multiple procedures with an Assessment and the same procedure can also be linked to multiple Assessments. Each procedure consists of a series of steps that must be performed in sequence.

Caution: Do not confuse Assessment Procedures with Audit Procedures. Audit Procedures provide detailed steps to be performed during audit fieldwork while Assessment Procedures are taken to assess control risk.

5. Record an Overall Opinion / Evaluation of the Assessment

| Topic | Navigation Path |
|--|--|
| Record an Overall Opinion and Evaluation of the Assessment | Navigate to the Audit Operations > Assessment tab and select the appropriate Assessment for which you enter an opinion and evaluation. |

The Evaluations page has two sections as follows:

1. Overall Opinion of the Assessment

Click the Update Opinions button to enter your Opinion of the Assessment and Components as well as your Comments. Note that only the Assessment owner (specified when the Assessment is created) can update the Overall Opinion section. Other users will not see the Update Opinions button.

The Assessment Owner generally enters this opinion after reviewing Evaluations of the Assessment and its components (described in the following point).

2. Evaluations

Click the Evaluate button to enter your Evaluation of the Assessment as well as the Components with respect to which the Assessment was made. You can also enter your comments.

The Lookup Type used for both the overall effectiveness of the Assessment as well as for the evaluation of components is AMW_EVALUATION_CONCLUSION. It has an accessibility level of User.

When Process owners are certifying their business processes, they can view all Assessments associated with those procedures.

Note: For more information on Process Certifications, refer to Process Certifications, page 10-1.

Restrictions

The amount of subsequent procedural work performed in an audit (testing of controls as well as other tests like tests of details of balances) depends to a large extent on an auditor's assessment of the organization's internal control structure and compliance with established controls and regulations.

If the up front assessment shows that the organization's internal control structure and overall compliance are highly effective, then auditors will tend to rely on this assessment and minimize the amount of audit field work.

The opinion and evaluation of the Assessment is therefore critical and sensitive data. In order to provide an appropriate level of security in the entering and update of Assessment Evaluations, Oracle Internal Controls Manager distinguishes between the following personnel:

- A User entering the assessment results (Entered By)
- An Evaluator who actually performs the assessment (Executed By)

The following restrictions apply to these two roles:

1. For any given Assessment, there can be no more than one evaluation per Evaluator.
2. A User with access to Assessment Evaluations can create multiple evaluations. As noted in point 1 above, each evaluation must have a different Evaluator.
3. Only the owner of an Assessment (specified when the Assessment is created) can enter and update the "overall opinion" section of the Assessment.
4. An existing evaluation can only be updated by the User who created (Entered) it and the Evaluator. To be updated, the Status of the evaluation must be "In Process."
5. An evaluation can only be created (the "Evaluate" button is enabled) when the Assessment Status is "Completed" or "In Process." You cannot enter an evaluation if the Assessment status is "Not Started" or "Archived."

Note: Once the assessment of the organization's internal control structure and compliance with established controls is complete, you can then begin audit procedures to test controls and details of balances as well as perform other substantive tests.

Audit Engagements

This chapter covers the following topics:

- Introduction
- Setup the Audit Engagement within Oracle Internal Controls Manager
- Setup the Audit Engagement through Integration with Oracle Projects
- Scoping the Audit Engagement
- Executing the Audit Engagement
- Opinions Framework in Oracle Internal Controls Manager

Introduction

Both internal and external auditors conduct risk-based audits to test the effectiveness of mitigating controls over business processes. The results of the audit form a basis upon which auditors can attest that internal controls are functioning as intended. These risk-based audits are usually managed as projects.

The audit engagement represents a compilation of audit assignments for the business entity and becomes the central repository of information on the audit. Engagements integrated with Oracle Projects can also contain information on the audit's time frame, staffing, etc. to help you manage your resources and budgets as well as the information on your audit results.

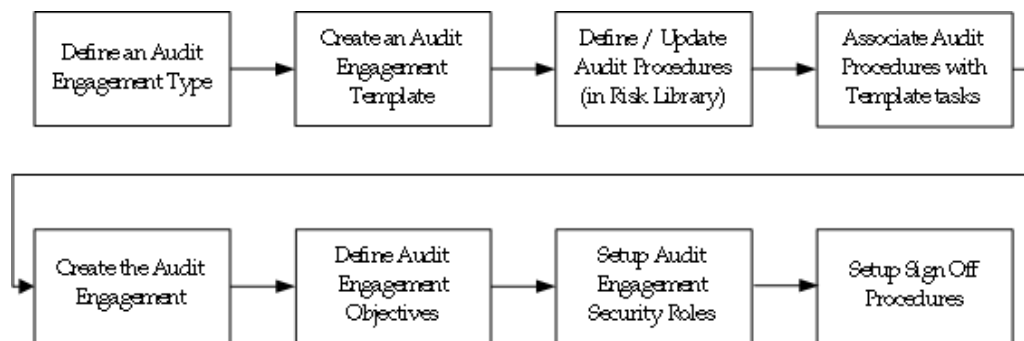
This chapter contains detailed information on setting up and executing your audit engagements.

Perform the followings tasks to create and implement your audit engagements:

- Set up the audit engagement There are two approaches that can be taken:
 - The audit engagement is setup within Oracle Internal Controls Manager itself.
 - The audit engagement is setup through an integration with Oracle Projects.
- Scope the audit engagement The engagement is scoped based on Company, Line of Business, Organization and Process.
- Execute the audit engagement The engagement is managed through Oracle Internal Controls Manager.

Setup the Audit Engagement within Oracle Internal Controls Manager

The following diagram shows a high level view of the steps that must be undertaken to set up an audit engagement.



1. Your first task is to create an Engagement Type.

| Topic | Navigation Path |
|---|---|
| Create an Engagement Type in Oracle Internal Controls Manager | Using the Internal Auditor (or equivalent) responsibility, navigate to the Setup tab and then the Engagements subtab to access the Type hyperlink |

Audit Engagements originate from Engagement Templates (or are copied from other engagements that in turn originated from templates). The templates in turn are linked to an Engagement Type.

Home Audit Operations Segregation of Duties Organizations Risk Library **Setup**

Engagements | Issue Management | Opinions | Risk Library | Regulations | Approvals | Value Sets

Setup: Engagements > Engagement Types >

Create Type

* Indicates required field

* Internal Name: SW_Internal_Audit

* Name: SW Internal Audit

Description: [Text Area]

* Start Date: 05-Apr-2005

End Date: [Date Picker]

☐ Set as Default Type

Project Type: [Dropdown]

Number Generation: [Dropdown]

Cancel Apply

The following table provides further information on select fields in the Create Type window.

| Field | Seeded Values | Description |
|-------------------|---|---|
| Project Type | All Project Types from Oracle Projects. | To setup the engagement within OICM, this field must be left blank. Note: If this field is entered, the value serves as a bridge to Oracle Projects. For more information on the setup of an Audit Engagement through integration with Oracle Projects, refer to the next section. |
| Number Generation | User Entered Sequence Generated | If User Entered, then a user enters a number manually when creating an Audit Engagement. You can also add a pre-fix for user entered numbers. For example, all IT audit projects start with prefix "ITA." |

You can define an unlimited number of extensible attributes when creating the Engagement Type. These attributes are displayed and available to all Engagements that are created using that particular Engagement Type.

Note: For more information on setting up and using Extensible Attributes, refer to Extensible Attributes in Oracle Internal Controls Manager, page 14-1.

2. Create Engagement Templates using this Audit Engagement Type.

| Topic | Navigation Path |
|---|--|
| Create an Engagement Template in Oracle Internal Controls Manager | Using the Internal Auditor (or equivalent) responsibility, navigate to the Setup tab and then the Engagements subtab to access the Templates hyperlink |

Engagement templates contain standard deliverables needed for the project. For example, the template will typically have standard auditing tasks for auditing a process as a part of the work breakdown structure of the project. Whenever an Engagement is created using this template, it will automatically include all of these tasks.

Create Template Tasks

Home

Audit Operations

Segregation of Duties

Organizations

Risk Library

Setup

Engagements | Issue Management | Opinions | Risk Library | Regulations | Approvals | Value Sets

Template: Investigation Template

Update

Template Name

Investigation Template

Number

Description

Type

Internal_Audit

Start Date

22-Feb-2005

End Date

Select Object:

Create Task

Expand All

Collapse All

⊕

| Select | Focus | Tasks | Number | Manager | Description | Update | Remove |
|-----------------------|-------|--------------------------|--------|---------|----------------|--------|--------|
| <input type="radio"/> | | ▼ Investigation Template | | | | | |
| <input type="radio"/> | | Fraud Controls | 10 | | Fraud Controls | | |
| <input type="radio"/> | | Credit Risk Analysis | 20 | | | | |

When a specific audit engagement needs to be undertaken, either as a scheduled activity or as the result of a trigger event (such as a large accounts receivable write off), the project is created from the appropriate template for the process or business flow being audited. As an example, if the process being audited is order to cash, the order to cash audit engagement template can be used to create the audit engagement.

Note that the audit of processes can require multiple audit engagement templates depending on the audit approach undertaken. In addition, different industries and time periods will require the use of different engagement templates for the same process.

Most audit tasks used to evaluate the risks and controls of the business process will originate in the engagement template but they can be also be created within the audit engagement.

3. Create/revise your audit procedures as part of the set up of the Risk Controls Library in Oracle Internal Controls Manager.

Note: For more information on creating audit procedures and audit procedure steps, refer to Setting up Audit Procedures in Oracle Internal Controls Manager, page 5-2.

4. Link audit procedures in the risk controls library with the tasks in an audit Engagement Template. Once associated, the audit procedures will be displayed with related tasks in all projects created from the Engagement Template.

There are two methods to link audit procedures with engagement template tasks.

METHOD 1

The following steps detail creating an enduring link between the template task and the audit procedure. Once realized, all projects created from this template will have tasks that are linked to these audit procedures.

To create this link, drilldown to the audit procedure details in the risk library.

| Topic | Navigation Path |
|---|---|
| Associate audit procedures with engagement template tasks | <p>Using the Internal Auditor (or equivalent) responsibility, click the Risk Library tab and then the Audit Procedures tab.</p> <p>For the relevant audit procedure click the Update icon to navigate to the Audit Procedure details window. Finally, go to the Audit Project Tasks subtab.</p> |

Home Audit Operations Segregation of Duties Organizations Risk Library Setup

Processes | Risks | Controls | **Audit Procedures** | Import

Risk Library: Audit Procedures > Select Classification >

Update Audit Procedure: Audit Procedures for Entering Supplier Invoices Controls >

Add Task: Audit Procedures for Entering Supplier Invoices Controls

* Indicates required field

* Template

Task:

Expand All | Collapse All

| Select Focus | Task Name | Task Number | Task Long Name |
|--------------|----------------------|-------------|----------------|
| | Root Node | | |
| | Fraud Controls | 10 | Fraud Controls |
| | Credit Risk Analysis | 20 | |

Once you select a template, project tasks from that template will be available to associate with the audit procedure. Select a task to link with the audit procedure.

As a result of this association, all audit engagements created from this engagement template will automatically have its project tasks linked to the relevant audit procedures in the Internal Controls Manager module.

METHOD 2

Using this method, you can create a link between the template task and the audit procedure for a particular engagement. The association is not set at the template level and consequently not valid for any other engagement.

| Topic | Navigation Path |
|---|---|
| Associate audit procedures with engagement template tasks | <p>Using the Internal Auditor (or equivalent) responsibility, navigate to the Audit Operations tab and then the Engagements subtab. Drill into the details of the appropriate Engagement and then go to the Tasks subtab.</p> <p>Drill into the required "Audit Procedures with No Task Assignments" and then Update it by adding a task.</p> |

In this way you link an audit procedure to the appropriate template task in this particular engagement.

Note the following with respect to the association of audit procedures with Engagement template tasks:

- An audit procedure can be associated with multiple tasks and vice versa.
- Audit procedures can be attached to a task in any template and at any level of the work breakdown structure. In most cases, this association will take place at the lowest level in the task hierarchy i.e. the work breakdown structure's leaf nodes.

5. Create the engagement from the appropriate Audit Engagement Template.

| Topic | Navigation Path |
|----------------------|--|
| Create an engagement | Using the Internal Auditor (or equivalent) responsibility, navigate to the Audit Operations tab and then the Engagements subtab. |

The screenshot shows the 'Create Engagement : Source List' form in the Oracle Internal Controls Manager. The navigation tabs at the top are Home, Audit Operations (selected), Segregation of Duties, Organizations, Risk Library, and Setup. Under 'Audit Operations', the subtabs are Engagements (selected), Assessments, Findings, and Remediation. The form title is 'Create Engagement : Source List'. Below the title, there is a note '* Indicates required field'. The 'Engagement Type' dropdown is set to 'Internal Audit'. There are two radio buttons: 'Create from Template' (which is selected) and 'Create from Engagement'. To the right of the 'Create from Engagement' radio button is a small icon of a hand pointing to a document. At the top right of the form are 'Cancel' and 'Continue' buttons.

In lieu of creating the project from a template, you may copy it from an existing engagement.

6. Setup Audit Engagement Security Roles

The application enables data security on Audit Engagements through the construct of "Roles." Roles allow users to have different data views and privileges on instances of objects (like Engagements) based on the data access rights of the role.

Note: For detailed information, refer to Roles and Privileges, page 15-1 and Function Security, page 16-1 in Oracle Internal Controls Manager. To use roles in the application, the profile option AMW: Implement Data Security must be set to "Yes."

Use the following menu path to setup Audit Engagement Security roles.

| Topic | Navigation Path |
|---|---|
| Engagement Security - Setup of Engagement Roles | Using the Internal Auditor (or equivalent) responsibility, navigate to the Audit Operations tab and then the Engagements subtab. Drill into the details of the appropriate Engagement and then go to the People subtab. |

Home Audit Operations Segregation of Duties Organizations Privileged Setup

Engagements Audit Engagements Engagement Audit Engagements

Audit Operations: Engagements > Audit Engagement: Americas: Americas: Audit Engagements

Update People

One record requires to be updated. [Cancel] [Apply]

Select People: [Default]

Select All | Select None

| Select Role | Type | Name | Company | Start Date | End Date |
|---|--------|----------|------------|-------------|----------|
| <input type="checkbox"/> Engagement and Manager | Person | John Doe | My Company | 12-Feb-2005 | |
| <input type="checkbox"/> [Dropdown] | Person | | My Company | 16-Apr-2005 | |

Add Another Row

TIP: Only for most companies: 05-Jul-2005

The application provides the following seeded roles with respect to executing Audit Engagements:

| Role | Privilege |
|---------------------|--|
| Engagement Approver | <p>Engagement approvers can "sign off" on Audit Engagements that are submitted to them.</p> <p>If the engagement is deemed to be satisfactorily completed, then Engagement Approvers approve the sign off. The Audit Engagement Status changes to "Signed Off" and the Sign off status becomes "Approved."</p> <p>If not acceptable, then the sign off is rejected. The Audit Engagement status remains "Active" and the Sign off status is changed to "Rejected."</p> <p>For more information, refer to Setup the Sign Off Process, page 8-9.</p> |
| Engagement Auditor | <p>Engagement Auditors are the primary executors of the Audit Engagement. Hence individuals with this role can add audit procedures and update their status (as well as the status of the individual steps that make up the audit procedure).</p> |
| Engagement Manager | <p>Engagement Managers scope the Audit Engagement and set security privileges in the application. The person who creates the Audit Engagement automatically gets this role.</p> <p>Engagement Managers can also execute the engagement.</p> |
| Engagement Reviewer | <p>Engagement Reviewers have view only access to the Audit Engagement.</p> |

While all users can create Audit Engagements, the Engagement Manager assigns a role to a "person" or to "All Users." You can assign multiple security roles to a person. Note that inherited roles are not valid for Audit Engagements.

7. Define the objectives of the Audit Engagement.

Audit Objectives provide a framework to help auditors plan their audits and decide on the proper evidence to accumulate. The objective is a powerful statement as to what you intend to achieve by executing the audit engagement. When a "Sign Off" (described subsequently) of the Audit Engagement is initiated, you can check whether the stated Audit Objectives were met.

| Topic | Navigation Path |
|-----------------------|---|
| Engagement Objectives | <p>Using the Internal Auditor (or equivalent) responsibility, navigate to the Audit Operations tab and then the Engagements subtab. Drill into the details of the appropriate Engagement and then go to the Objectives subtab.</p> <p>Click the Create button to define a new objective and the Add button to link previously defined objectives.</p> |

Home | **Audit Operations** | Segregation of Duties | Organizations | Risk Library | Setup

Engagements | Assessments | Findings | Remediation

Audit Operations: Engagements > Audit Engagement Americas Sales Audit Q1 2005 > Audit Objectives Details >

Update Audit Objectives

Cancel Apply

* Audit Objective: Assess Risk Exposure

* Audit Objective Type: Authorization

Description:

Control Components

Select All | Select None

| Select Control Components |
|--|
| <input type="checkbox"/> Control Activities |
| <input checked="" type="checkbox"/> Internal Environment |
| <input type="checkbox"/> Event Identification |
| <input type="checkbox"/> Information and Communication |
| <input type="checkbox"/> Monitoring |
| <input type="checkbox"/> Objective Setting |
| <input type="checkbox"/> Risk Assessment |
| <input type="checkbox"/> Risk Response |

| *Application Name | *Performance Measure Name | Delete |
|-------------------|---------------------------|--------|
| No data exists. | | |
| Add Another Row | | |

Audit Objective Type

You can declare the Type of Audit Objective. Seeded values are:

- Cut Off
- Authorization
- Completeness
- Accuracy
- Timely

These values are based on the Lookup Type AMW_AUDIT_OBJECTIVE and you can add/update the list as required.

Control Components

These are the predefined components affecting the organization's audit environment. The seeded components are from the COSO framework and you may classify the Audit Engagement objective as being associated with one of them.

Performance Measures

Audit objectives, when used in conjunction with process definitions, can also provide useful benchmarks to auditors for evaluating the performance of their audits. To this end the application allows you to associate Key Performance Indicators with the objective.

8. Setup a Sign Off Process (Optional)

You may optionally choose to implement a sign off for any of your Audit Engagements. When complete, the sign off process is initiated by submitting the Engagement for approval. One or more designated approvers will then have to approve the completion of the Engagement to change its status to "Signed Off / Complete." Sign off approval allows an additional level of security on highly sensitive engagements.

Note: By default, no sign off is required for Audit Engagements.

The sign off takes the form of a template with an unlimited number of extensible attributes that you can define based on the "Sign Off Type." These attributes will be displayed to approvers when the Engagement is submitted for sign off (for all Engagements created using that particular Sign Off Type). The routing of the sign off to the appropriate approvers is also determined by the Sign Off Type.

Perform the following steps to setup the Engagement's Sign Off capability:

Step 1: Define Audit Engagement Sign Off Types

| Topic | Navigation Path |
|--------------------------------|--|
| Setup Engagement Sign Off Type | Using the Internal Auditor (or equivalent) responsibility, navigate to the Setup tab and then the Engagements subtab to access the Engagement Sign Off Type. Setup all required extensible attributes and the approval template for the Sign Off Type. Note that all users on the approval template can sign off on engagements even if they are not given the "Engagement Approver" role. |

Note: For more information on setting up and using Extensible Attributes associated with the Sign Off Type, refer to Extensible Attributes in Oracle Internal Controls Manager, page 14-1.

Step 2: Initiate the Sign Off Approval Requirement

| Topic | Navigation Path |
|---------------------------------|---|
| Engagement Sign Off Requirement | Using the Internal Auditor (or equivalent) responsibility, navigate to the Audit Operations tab and then the Engagements subtab. Drill into the details of the appropriate Engagement. Click the update button to set whether Sign Off Approval is required. |

Note: The process of submitting the Audit Engagement object for Sign Off is fully described in the section Execute the Audit Engagement.

For Sign Offs to be active, Business Event Processing must be enabled.

Setup the Audit Engagement through Integration with Oracle Projects

Oracle Internal Controls Manager is fully integrated with Oracle Projects so that the risk-based audit engagement can be created and managed in the same fashion as any other project. While the management of the project is done in Oracle Projects, scoping of the project and the project's fieldwork evaluation is managed through the Oracle Internal Controls Manager application.

By creating your audit engagement as a project in Oracle Projects, you leverage the many features of the Oracle Projects suite of applications. Oracle Project Applications – a component of Oracle's E-Business Suite – provides these benefits by enabling you to streamline your business projects. As a result, you can run your audit engagements in a more efficient and effective way.

The following project modules can be used with Oracle Internal Controls Manager for project integrated engagements:

Oracle Project Management: Oracle Project Management provides audit managers the ability to manage audit engagements through the project life-cycle from planning, through execution, to completion. As it is a fully integrated module within the Oracle Projects family, audit managers can look to a single source of enterprise project information for all their needs.

The application provides features like audit workplan, resource assignments, financial forecasts, document management, project accounting, communications to stakeholders, and collaborative execution of project work internal and external to the organization.

Oracle Project Resource Management: Once the audit engagement is created, it must be sourced. Before assigning work, managers need to review the audit department's workload and capacity. Oracle Project Resource Management can be used by audit managers to locate and deploy qualified resources to staff their projects across the enterprise.

The application enables you to get a snapshot of resources and their availability – available resources, over-committed resources, etc. -- through a portal. Workflow technology notifies the audit manager of events requiring action, such as candidate nominations and assignment approvals.

Oracle Project Costing: Oracle Project Costing provides a complete and integrated cost management solution for all your audit engagements. You can effectively manage these projects even if they cross currency and organizational boundaries. Oracle Project Costing provides internal audit managers with access to timely, detailed cost information to monitor audit procedures while financial managers can track the total cost of running the projects.

In the Project Costing module, audit engagements can be broken up into underlying tasks (a work breakdown structure). You can then create a budget, based on an estimate of the resources required to complete the tasks. As employees work on the tasks in an audit engagement, they create expenditures to reflect the project costs they incur. As costs are incurred, you can compare them with your budget to track the audit engagement's progress.

Oracle Project Costing acts as a central repository of project transactions, processes project costs and creates corresponding accounting entries for your Corporate Finance Department, based upon accounting rules.

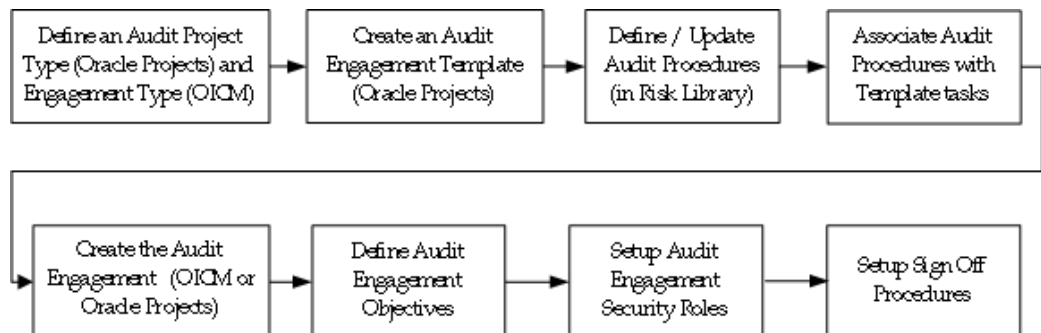
Oracle Project Intelligence: Oracle Project Intelligence can serve as a comprehensive analysis and reporting solution for all audits that are set up as projects. Oracle Project Intelligence provides essential project-based operational and financial metrics directly to audit managers and other stakeholders.

Through role-based portals, audit managers have access to information regarding the state of their projects relative to various performance measures. This real-time view allows the stakeholders of the audit engagement to stay informed, develop insight, and take action.

Audit engagements can be monitored for progress against milestones using Oracle's Project Intelligence projects. Large portfolios of projects can be monitored for degree of completion by phase or towards a particular milestone.

Setup the Oracle Projects Integrated Audit Engagement

The following diagram shows a high level view of the steps that must be undertaken to set up this audit engagement.



Note: Several of these setup steps are performed in Oracle Projects. Refer to the appropriate Oracle Projects documentation for more details.

1. Your first task is to create an "Audit" Project Type (Engagement Type) in Oracle Projects. This Project Type must be seeded within the Oracle Internal Controls Manager application as follows:

| Topic | Navigation Path |
|---|---|
| Create an Engagement Type in Oracle Internal Controls Manager | Using the Internal Auditor (or equivalent) responsibility, navigate to the Setup tab and then the Engagements subtab to access the Type hyperlink |

The screenshot shows the 'Create Type' window in Oracle Internal Controls Manager. The window has a title bar with tabs: Home, Audit Operations, Segregation of Duties, Organizations, Risk Library, and Setup. Below the title bar is a navigation bar with links: Engagements, Issue Management, Opinions, Risk Library, Regulations, Approvals, and Value Sets. The main content area is titled 'Create Type' and contains the following fields:

- * Internal Name: SW_Internal_Audit
- * Name: SW Internal Audit
- Description: (empty text area)
- * Start Date: 05-Apr-2005
- End Date: (empty date field)
- ☐ Set as Default Type
- Project Type: (dropdown menu)
- Number Generation: (dropdown menu)

There are 'Cancel' and 'Apply' buttons at the top right of the window.

The following table provides further information on select fields in the Create Type window.

| Field | Seeded Values | Description |
|--------------|---|---|
| Project Type | All Project Types from Oracle Projects. | When you select one of these values for Project Type, then the value serves as a "bridge" to Oracle Projects i.e. it becomes an "Oracle Projects" engagement, created in Oracle Projects. |

For more details, refer to the corresponding step under Setup the Audit Engagement within Oracle Internal Controls Manager

2. In Oracle Projects, create project (engagement) templates using this Audit Engagement Type. Note that all projects in Oracle Projects are created from templates (or copied from other projects that in turn originated from templates). However, only projects created from templates with the Audit Project Type will appear as engagements in Oracle Internal Controls Manager.

Most audit tasks used to evaluate the risks and controls of the business process will originate in the project template but they can be also be created within the audit engagement.

3. Create/revise your audit procedures as part of the set up of the risk controls library in Oracle Internal Controls Manager.

Note: For more information on creating audit procedures and audit procedure steps, refer to Setting up Audit Procedures in Oracle Internal Controls Manager, page 5-2.

4. Link audit procedures in the risk controls library with the tasks in an audit engagement template (Even though created in Oracle Projects, the template will also display in Oracle Internal Controls Manager). Once associated, the audit procedures will be displayed with related tasks in all projects created from the audit engagement template.

For more details, refer to the corresponding step under Setup the Audit Engagement within Oracle Internal Controls Manager.

5. Create the audit engagement from the appropriate audit engagement template in Oracle Projects or in Oracle Internal Controls Manager. In lieu of creating the project from a template, you may copy it from an existing audit engagement (one that has an Audit Engagement Type).

For more details on creating the engagement within OICM, refer to the corresponding step under Setup the Audit Engagement within Oracle Internal Controls Manager.

6. Setup Audit Engagement Security Roles

For more details, refer to the corresponding step under Setup the Audit Engagement within Oracle Internal Controls Manager

7. Define the objectives of the Audit Engagement (Optional)

For more details, refer to the corresponding step under Setup the Audit Engagement within Oracle Internal Controls Manager

8. Setup a Sign Off Process (Optional)

For more details, refer to the corresponding step under Setup the Audit Engagement within Oracle Internal Controls Manager

9. Finally, complete your project set up in Oracle Projects. This will include, but not limited to, establishing the following parameters in the project:

- Resources and key members
- Costing information and distribution rules
- Organizations
- Project status

Though the project status is not relevant to Oracle Internal Controls Manager, critical functionality within Oracle Projects modules is dependent on the status of a project.

Note: For more information, refer to the appropriate Oracle Projects documentation.

Scoping the Audit Engagement

After creating the audit engagement, your next task is to define its scope. In Oracle Internal Controls Manager, the scope determines which entities and processes are included in the project and therefore defines the context in which audit procedures are executed. The scope of the audit engagement provides boundaries to the execution of the audit. Once the scope is resolved, an auditor can finalize the audit procedures that comprise the audit engagement.

There are two ways to define the scope of the audit engagement in Oracle Internal Controls Manager:

- Using Companies, LOB's, Organizations and Processes
- Using Organizations and Processes only

Scoping with Companies, LOB's, Organizations, and Processes

| Topic | Navigation Path |
|------------------------|--|
| Audit Engagement Scope | <p>Using the Internal Auditor (or equivalent) responsibility, navigate to the Audit Operations tab and then the Engagements subtab. Drill into the details of the appropriate Engagement and then go to the Scope subtab.</p> <p>Click the Add to Scope button to activate the scope wizard.</p> |

Use the wizard to define the audit engagement scope as follows:

1. Select the companies you wish to add to the project scope.



2. Select the lines of businesses (LOBs) within the companies chosen in the previous step.

All lines of businesses within the selected companies can be activated. When selecting lines of businesses, you may choose to include parents only or parent and children lines of businesses. Oracle Internal Controls Manager provides a checkbox to include auditable units within the companies selected that have no line of business assignments.

Note: Companies and lines of businesses are linked to auditable units in the HR organizations window. For more information, refer to Organizations in Oracle Internal Controls Manager, page 2-29.

3. Include additional organizations (auditable units) in the project scope. The "Scope: Include Organizations" window shows a leading and trailing list of organizations. By default, the leading list is empty and the trailing list shows the organizations that belong to the selected companies and LOBs. A filter on

organization name is included in the leading list and you can search for additional organizations to be included in the scope.

Note: If security is turned on, then you can only include into scope those orgs on which you have "Audit Organization" privilege.

For more information, refer to Roles and Privileges in Oracle Internal Controls Manager, page 15-1.

You may also remove from the audit engagement scope any organizations that are included based on the selected companies and lines of businesses.

4. Include relevant processes

Oracle Internal Controls Manager uses the combination of company, lob, and organization to provide a subset of auditable units from which processes can be selected. All first level parent processes belonging to auditable units within the selected combination of subsidiaries, lobs, and organizations will be displayed.

Note: You may later choose to exclude particular child processes under a parent process. To do this, click the Manage Included Processes icon associated with a particular auditable unit in the scope details window.

5. Once you have selected the parent processes to be included, click the submit button in the wizard to create the audit engagement scope.

Scoping with Organizations and Processes only

| Topic | Navigation Path |
|------------------------|--|
| Audit Engagement Scope | Using the Internal Auditor (or equivalent) responsibility, navigate to the Audit Operations tab and then the Engagements subtab. Drill into the details of the appropriate Engagement and then go to the Scope subtab. Click the Add Organizations button to activate the scope wizard. |

1. Though you can enter the Company and LOB fields to narrow down the Organizations, this method of scoping is generally used to directly enter the appropriate organizations (auditable units) into the project scope. The "Add Scope: Include Organizations" window shows a leading and trailing list of organizations. A filter on organization name is included in the leading list and you can search for additional organizations to be included in the scope.

Note: If security is turned on, then you can only include into scope those orgs on which you have "Audit Organization" privilege.

For more information, refer to Roles and Privileges in Oracle Internal Controls Manager, page 15-1.

2. Include relevant processes

All first level parent processes belonging to organizations (auditable units) selected will be displayed.

Note: You may later choose to exclude particular child processes under a parent process. To do this, click the Manage Included Processes icon associated with a particular auditable unit in the scope details window.

Once you have selected the parent processes to be included, click the submit button in the wizard to create the audit engagement scope.

The scope details window now displays the entities (companies, LOBs, organizations) and processes in the audit engagement scope. Auditable units (and processes) within the companies selected but not associated with a line of business are displayed under the node "Auditable Units with No Line of Business Assignments."

Home Audit Operations Segregation of Duties Organizations Risk Library Setup

Engagements Assessments Findings Remediation

Audit Operations: Engagements >

Audit Engagement: Americas Sales Audit Q1 2005

Update

Report AMW Audit Report Generate View

Type Internal Audit Type

Sign Off Status Not Submitted

Description

Name Americas Sales Audit Q1 2005

Number IA10024

Manager Sharma, Anita

Status Active

Start Date 12-Feb-2005

View Main

Objectives Scope Tasks Controls Risks Processes Organizations Findings Attachments Se

View Legal Hierarchy Add to Scope Add Organizations

Expand ICM HR Org Hierarchy

Legal Hierarchy

Management Hierarchy

| Focus | Organization | Type | Location | Manage Included Processes | Remove |
|-------|--------------------------|----------------|---------------|---------------------------|--------|
| | Root Node | | | | |
| | North America Operations | | | | |
| | Vision Enterprise | Company | New York City | | |
| | US Operations | | | | |
| | Vision Computers | Operating Unit | | | |

Notes on Scoping

Hierarchical Views

You can now view the engagement scope through a hierarchical filter. Three hierarchy views are available:

1. Custom Hierarchy. This is the hierarchy of organizations as defined in the Oracle HR module and entered in the "AMW: Org Security Hierarchy" profile option.
2. Legal Hierarchy. This is the hierarchy of subsidiaries (companies) in the Subsidiary Value Set. The value set name must be entered in the "AMW: Subsidiary Value Set for Audit Units" profile option.
3. Management Hierarchy. This is the hierarchy of LOB's in the LOB Value Set. The value set name must be entered in the "AMW: LOB Value set for Audit Units" profile option.

Viewing the Tasks and Procedures in Scope

| Topic | Navigation Path |
|---------------------|--|
| Audit Tasks Details | <p>Using the Internal Auditor (or equivalent) responsibility, click the Audit Operations tab and then the Engagements subtab.</p> <p>Drill down into audit details of the appropriate engagement and then click the Audit Tasks hyperlink.</p> |

The tasks originate in the engagement template and are typically the ones you want to reuse. They appear linked to their associated procedures in the Audit Tasks Details window.

However, there may be audit procedures related to processes in entities that have been included in an expanded scope, but not yet associated with project tasks. These procedures appear under the dummy node "Audit Procedures with no Task Assignments."

Home

Audit Operations

Segregation of Duties

Organizations

Risk Library

Setup

Engagements

Assessments

Findings

Remediation

Audit Operations: Engagement Info

Audit Engagement: Americas Sales Audit Q1 2005

Update

Name: Americas Sales Audit Q1 2005

Summary: 1A10024

Manager: Shamini, Anita

Owner: Arlene

Start Date: 12-Feb-2005

Report: AMW Audit Report

Generate

View

Update

Type: Internal Audit

Typical Feature: Not Submitted

Description:

View: Main

Objectives

Scope

Tasks

Controls

Issues

Processes

Organizations

Findings

Alerts/Events

Settings

Help

(Add Task) (Download)

Expand All | Collapse All

| Select | Focus | Tasks | Organization | Status | By | Executed | Executed On | Open Findings | Add Audit Procedure | Create and Add Audit Procedure | Copy | Move | Update | Remove |
|--------|-------|---|--------------|-------------|----|----------|-------------|---------------|---------------------|--------------------------------|------|------|--------|--------|
| | | Americas Sales Audit Q1 2005 | | | | | | | | | | | | |
| | | Audit Procedures with no Task Assignments | | | | | | | + | | | | | |
| | | Particular: vision Columns: Computers Audit Procedure | | Not Started | | | | | | | | | | |

Modify the Task List

You can modify the task list by performing the following operations in this window:

- Add audit procedures to tasks. You may also create new audit procedures (through the "Create and Add Audit Procedures" feature) that are unique to this engagement.

Note: For more information, refer to the section Creating Audit Procedures within Audit Engagements, page 5-6.

- Copy existing audit procedures to other tasks
- Move audit procedures between tasks
- Remove audit procedures from being associated with tasks. Once removed, these procedures are eliminated from the audit engagement scope.

Note that if you delete a task in the engagement template, its associated audit procedures are transferred to the "Audit Procedures with no Task Assignments" node. Use the "Move to Task" icon to associate these procedures with alternate tasks.

Note: Update the status of the audit procedure by clicking the Status hyperlink associated with the Audit Procedure.

Creating Audit Procedures within the scope of an Audit Engagement

In addition to the usual method of creating or importing Audit Procedures in the Risk Library, you can also create Audit Procedures within the course of an Audit

Engagement. The requirement for running these procedures will normally arise during the course of the engagement.

Note: For a detailed introduction to Audit Procedures, refer to Audit Procedures in Oracle Internal Controls Manager, page 5-1.

The application hence allows you to create them ad hoc within an engagement and all such procedures are specific to the engagement they are created in. These procedures are not visible in the application's risk library or while working with other Audit Engagements.

| Topic | Navigation Path |
|---------------------|--|
| Audit Tasks Details | <p>Using the Internal Auditor (or equivalent) responsibility, click the Audit Operations tab and then the Engagements subtab.</p> <p>Drill down into audit details of the appropriate engagement and then click the Audit Tasks hyperlink.</p> <p>Finally click the "Create and Add Audit Procedure" icon.</p> |

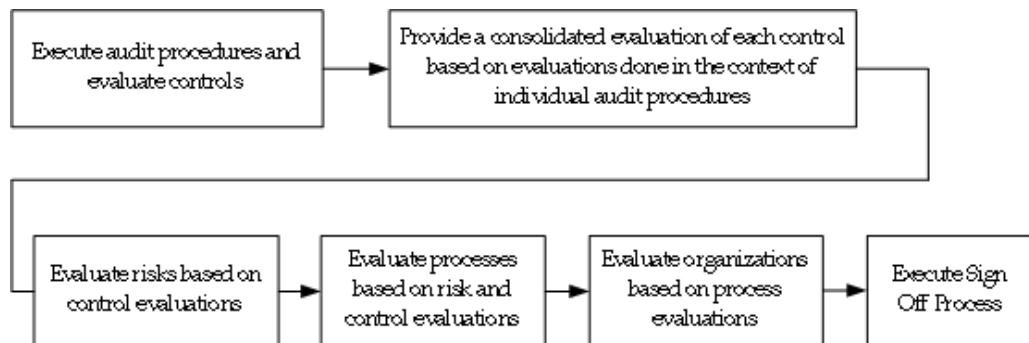
You may use all the regular features of Audit Procedures when completing the definition of these procedures. For example, you can define an unlimited number of extensible attributes which are available for use with the procedure.

Note: For more information on setting up and using Audit Procedure Classifications and Extensible Attributes, refer to Extensible Attributes in Oracle Internal Controls Manager, page 14-1.

Search feature for Audit Engagement Procedures

Click the Audit Procedure icon under the Tasks window to search for Audit Engagement procedures to add to scope.

Executing the Audit Engagement



Auditors document the results of their fieldwork based on the completed audit tasks, procedures, and steps. Audit evaluations can be documented for controls, risks, processes, and organizations within the scope of the audit engagement.

These evaluations are typically made in terms of "opinions" you can enter to record the results of the audit engagement. The application is pre-seeded with audit opinion values for each of the objects (audit procedure controls, organization controls, process risks, processes, organizations) being evaluated.

Note: You can also choose to set up user defined values for audit opinions. For more information, refer to the Opinions Framework in Oracle Internal Controls Manager, page 8-29.

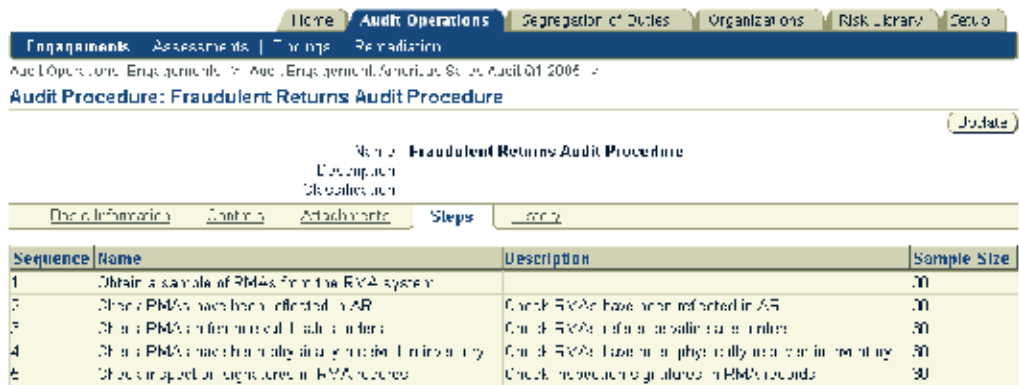
During the execution of the audit, nonconformities to established standards are logged as "Findings." A process certification cannot be issued until these Findings are effectively addressed and remedied.

Note: For more information on creating Findings, refer to Findings in Oracle Internal Controls Manager, page 12-1.

Step 1: Execute individual audit procedures (associated with Tasks) and evaluate individual controls

Execute Audit Procedures

| Topic | Navigation Path |
|-------------------------|--|
| Audit Procedure details | Using the Internal Auditor (or equivalent) responsibility, click the Audit Operations tab and then the Engagements subtab. Drilldown into the appropriate engagement and click the Audit Tasks hyperlink. Drilldown into a task and then into the audit procedures linked to the task. Execute the audit procedure according to the Steps listed. |



Evaluate Individual Controls

| Topic | Navigation Path |
|----------------------|--|
| Record audit results | Using the Internal Auditor (or equivalent) responsibility, click the Audit Operations tab and then the Engagements subtab. Drilldown into the appropriate engagement and click the Controls hyperlink. Drilldown into a Control to view and evaluate the audit procedures linked to that Control. |

The screenshot shows the Oracle Internal Auditor interface. At the top, there are tabs for 'Engagements', 'Audit Operations', 'Design and Build', 'Operational', 'Security', and 'Help'. The 'Audit Operations' tab is selected, and the 'Engagements' subtab is active. The main heading is 'Audit Engagement: Americas Sales Audit Q1 2005'. Below this, there are fields for 'Name', 'Status', 'Sign Off Required', 'Message', and 'Type'. The 'Name' field is set to 'Americas Sales Audit Q1 2005', 'Status' is 'Active', 'Sign Off Required' is 'No', 'Message' is 'Summary Audit', and 'Type' is 'Internal Audit type'. There are also fields for 'Report', 'Run by', 'Start Date', 'Sign Off Status', and 'Description'. The 'Report' field is set to 'Audit Report', 'Run by' is 'IA30024', 'Start Date' is '12 Feb 2006', 'Sign Off Status' is 'Not Submitted', and 'Description' is empty. Below these fields, there is a 'View' dropdown menu set to 'List'. The main table has columns for 'Details', 'Control', 'Description', 'Organization', 'Type', 'Automation', 'Control Location', 'Key Control', 'Open Findings', 'Evaluation', 'Evaluation History', and 'Evaluate'. The 'Evaluate' column contains icons for evaluating each procedure. The table shows three rows of audit procedures: 'Evaluation of Sales', 'Evaluation of Sales', and 'Evaluation of Sales'. Each row has a 'Details' column, a 'Control' column, a 'Description' column, an 'Organization' column, a 'Type' column, an 'Automation' column, a 'Control Location' column, a 'Key Control' column, an 'Open Findings' column, an 'Evaluation' column, an 'Evaluation History' column, and an 'Evaluate' column. The 'Evaluate' column contains icons for evaluating each procedure.

Audit procedures executed in the project test the effectiveness of particular controls. Click the Evaluate Control icon associated with the individual audit procedures to enter these control evaluations. The evaluation of the controls that the audit procedure is associated with is made regarding:

- Design Effectiveness
- Operating Effectiveness
- Finally enter an overall conclusion for the control (associated with the individual audit procedure) based on the audit procedure executed.

| Field | Seeded Values | Source | Accessibility Level |
|----------------------------|--|---|---|
| (Audit Opinion) Conclusion | Effective Deficient Significantly Deficient Materially Weak | Opinions Framework components for the Organization - Audit Procedure - Control object: * Audit Opinion * Design Effectiveness * Operating Effectiveness | Refer to the section: Opinions Framework in Oracle Internal Controls Manager, page 8-29 |

You can also create Findings that are associated with individual Audit Procedures.

Note - once this is done, you can change the status of the procedure from "Not Started" to "In Progress" and then "Completed with Issues" or "Completed".

Update Audit Procedure status

You can at any time update the status of the audit procedure by clicking the Status hyperlink associated with the Audit Procedure.

Enter Results through the "Download" and "Upload" facility

Click the Download button in the Tasks window to download the whole task structure with its audit procedures.

The screenshot shows the Oracle Internal Controls Manager interface. At the top, there are tabs for Home, Audit Operations, Segregation of Duties, Organization, Risk Library, and Setup. Below these are sub-tabs for Engagements, Assessments, Findings, and Remediation. The main window is titled 'Audit Engagement: AmerSales01'. It contains a header with buttons for Start, Sign Off, and Update. Below the header, there are fields for Name (AmerSales01), Status (Active), Sign Off Required (No), Manager (A Bakker), Type (Internal Audit), Report (AMM Audit Report), Number (505), Start Date (22 May 2005), Sign Off Status (Not Submitted), and Description (AmerSales up001). There are buttons for Generate and View. Below this is a 'Tasks' tab with a 'Download' button. A table lists tasks with columns for Select, Focus Tasks, Organization, Status, By, Executed, Executed On, Findings, Procedure, Add Audit, Create and Add Audit, Procedure Copy, Move, Update, and Remove. The tasks listed are 'Audit Procedures with No Task Assignments', 'Default Task', and 'Credit Authorization'.

You can evaluate the structure in MS Excel and then use the Oracle > Upload facility in Web ADI to upload the results back to the engagement. Note that only the Evaluation results (Design Effectiveness, Operating Effectiveness and Audit Opinion are uploaded; changes made to the rest of the spreadsheet are ignored).

Step 2: Provide a consolidated evaluation of the control

| Topic | Navigation Path |
|----------------------|--|
| Record audit results | Using the Internal Auditor (or equivalent) responsibility, click the Audit Operations tab and then the Engagements subtab. Dilldown into the appropriate engagement and click the Controls hyperlink. |

All controls associated with risks and processes in the audit engagement scope are listed in this window. There will typically be multiple audit procedures associated with a particular control. Clicking the Show Details icon displays the results of all the individual audit procedures associated with and undertaken to evaluate that control.

Click the Evaluate icon to record your consolidated evaluation of the control based on the individual audit procedures undertaken (as described in Step 1).

- In the following Evaluate Control window, click the Risks Mitigated hyperlink to view the risks associated with the control being evaluated. This view provides context on all the risks that the control is mitigating and assists in your final audit opinion of the control.
- Click the Control Evaluation hyperlink to enter a consolidated evaluation of the control. This evaluation is also made regarding:
 - Design Effectiveness
 - Operating Effectiveness

Oracle Internal Controls Manager requires you to enter an overall audit opinion with respect to the particular control based on the audit procedures undertaken.

| Field | Seeded Values | Source | Accessibility Level |
|-------------------------------|---|---|---|
| (Audit Opinion) Conclusion | Effective Deficient Significantly Deficient Materially Weak | Opinions Framework components for the Organization - Control object: * Audit Opinion * Design Effectiveness * Operating Effectiveness | Refer to the section: Opinions Framework in Oracle Internal Controls Manager, page 8-29 |

Note: It is important to remember that this evaluation is a summary evaluation of the control and consolidates the individual control evaluations made while entering the results of audit procedures in Step 1.

Step 3: Evaluate risks based on evaluations of the controls mitigating those risks

| Topic | Navigation Path |
|----------------|--|
| Evaluate Risks | Using the Internal Auditor (or equivalent) responsibility, click the Audit Operations tab and then the Engagements subtab. Drilldown into the appropriate engagement and click the Risks hyperlink. . |

Oracle Internal Controls Manager

Audit Operations | Engagement | Findings | Audit Plan

Audit Engagement: Americas Sales Audit Q1 2004

Engagement: Americas Sales Audit Q1 2004
Engagement Number: 1001
Status: Active

Report: **ACCM Audit Report** | Generate | View
Run Date: 01-Jan-2004
Engagement Manager: Frazier, Mr. London
Risk C# Status: Not Submitted

Audit Objectives | **Secs** | **Audit Tasks** | **Controls** | **Risks** | **Processes** | **Organizations** | **Findings** | **Attachments** | **Set**

Details | Risk | Organization | Process | Open Findings | Evaluation | Evaluation History | Evaluate

▼ In: Unauthorized Processing of Supplier Invoices | Sales LT02 | Primavera Pay | | [Conceal Mitigated](#) | |

Controls

| Control | Description | Type | Automation Type | Control Location | Open Findings | Evaluation | Evaluation History | Evaluate |
|--|---|-----------|--------------------|------------------|---------------|------------|--------------------|----------|
| Access to functions of data is restricted | Access to invoice processing functions is restricted to authorized personnel. Privileges are granted from incompatible roles. | Automatic | Application Access | Global | | | 00% | |
| Access is automatically terminated when employee is terminated | Workflow automatically ends user access when an employee is terminated. | Automatic | Workflow | Global | | | 00% | |

All risks associated with processes in the audit engagement scope are listed in this window.

There can be multiple controls mitigating this risk that are associated to the risk. Clicking the Show Details icon displays the details of all the individual controls associated with and undertaken to mitigate the risk.

Click the Evaluate icon to record your evaluation of the risk based on your evaluations of the controls mitigating the risks (as described in Step 2).

- In the following Evaluate Risk window, click the Risk Processes hyperlink to view all the processes that are exposed to the risk being evaluated. This view provides a process context and can assist in your final audit opinion of the risk.
- Click the Risk Evaluation hyperlink to enter an overall audit opinion with respect to the particular risk.

| Field | Seeded Values | Source | Accessibility Level |
|----------------------------|--|---|---|
| (Audit Opinion) Conclusion | Mitigated Somewhat Mitigated Somewhat Exposed Fully Exposed | Opinions Framework "Audit Opinion" component for the Organization - Process - Risk object | Refer to the section: Opinions Framework in Oracle Internal Controls Manager, page 8-29 |

Step 4: Evaluate processes based on risk and control evaluations

| Topic | Navigation Path |
|--------------------|--|
| Evaluate Processes | <p>Using the Internal Auditor (or equivalent) responsibility, click the Audit Operations tab and then the Engagements subtab.</p> <p>Drill down into the appropriate engagement and click the Processes hyperlink.</p> |

Home | Audit Operations | Segregation of Duties | Organizations | Risk Library | Setup

Engagements | Assessments | Findings | Remediation

Audit Operations > Engagements >

Audit Engagement: Americas Sales Audit Q1 2004

Update

Report

Audit Summary

Generate

View

Engagement

Americas Sales Audit Q1 2004

Start Date

01 Jan 2004

Prepared By

Ernie, M. London

Sign Off Status

Not Started

Engagement

Americas Sales Audit Q1 2004

Engagement Number

1001

Action

Audit Objectives

Scope

Audit Tasks

Controls

Tasks

Processes

Organizations

Findings

Attachments

View

Organization Processes Summary

Select Organization

Focus

| Focus Name | Open Findings | Risks | Controls | Evaluation Result | Evaluation History | Evaluate |
|----------------------------|---------------|-------|----------|-------------------|--------------------|----------|
| ▼ Enterprise | | | | | | |
| ○ ► Vision Corporation | | | | | | |
| ↻ ▼ Engagement 1001 | | | | | | |
| ○ ► Sales Order Management | | 1/14 | 0/07 | | | |
| ↻ ► Sales 1002 | | | | | | |
| ↻ ▼ Sales 1003 | | | | | | |
| ► Pension Plan Pay | | 0/11 | 0/12 | | | |

All processes and entities (companies, lines of business, and auditable units) in the audit engagement scope are available and you can view either:

- A list of processes or
- Processes according to the Organization Process hierarchy

Click the Evaluate icon for the relevant process to record your evaluation of the process based on your evaluations of the following:

- The risks that the process is exposed to (as described in Step 3)
- The controls mitigating those process risks (as described in Step 2)

In the Evaluate Process window enter an overall audit opinion for the process.

| Field | Seeded Values | Source | Accessibility Level |
|-------------------------------|--|---|---|
| (Audit Opinion) Conclusion | Effective Deficient Significantly Deficient Materially Weak | Opinions Framework "Audit Opinion" component for the Organization - Process object. | Refer to the section: Opinions Framework in Oracle Internal Controls Manager, page 8-29 |

Step 5: Evaluate organizations based on process evaluations

| Topic | Navigation Path |
|------------------------|--|
| Evaluate Organizations | Using the Internal Auditor (or equivalent) responsibility, click the Audit Operations tab and then the Engagements subtab. Dilldown into the appropriate engagement and then click the Organizations hyperlink. |

The screenshot shows the Oracle Internal Controls Manager interface. The top navigation bar includes tabs for 'Engagements', 'Assessments', 'Findings', 'Recommendation', 'Audit Operations', 'Segregation of Duties', 'Organizations', 'Risk Library', and 'Reports'. The 'Organizations' tab is selected. Below the navigation bar, the 'Audit Operations' subtab is active, showing the 'Americas Sales Audit Q1 2004' engagement. The engagement details include 'Engagement Number: 1001', 'Status: Active', 'Report: Show Audit Report', 'Start Date: 01-Jan-2004', 'Engagement Manager: Frazee, Mr. Landon', and 'Sign Off Status: No Sign Off'. The 'Organizations' tab is selected, displaying a hierarchical tree on the left and a table of organizations on the right. The table has columns for 'Inactive', 'Inactive Investigated', 'Inactive Open', and 'Evaluation'. The table lists organizations such as 'Vista Corporation', 'Empire State Building', and 'Sales, HRP'.

| Organization | Type | Location | Inactive | Inactive Investigated | Inactive Open | Evaluation |
|-----------------------|-----------|---------------------|----------|-----------------------|---------------|------------|
| Vista Corporation | Corporate | HQ - New York | 1/1/00 | 1/1/03 | 1/1/03 | Deficient |
| Empire State Building | Corporate | NYC - New York City | 1/1/00 | 1/1/03 | 1/1/03 | Deficient |
| Sales, HRP | Corporate | NYC - New York City | 1/1/00 | 1/1/03 | 1/1/03 | Deficient |

Note that you can view the Organizations through the hierarchical filter described earlier.

Click the Evaluate icon for the appropriate Auditable Unit. The evaluation of the organization is based on the evaluation of the processes being executed in that organization. In accordance with COSO standards, this evaluation is made with respect to the five COSO components:

- Control Environment
- Risk Assessment
- Control Activities
- Information and Communication
- Monitoring

Based on the above evaluation, you can enter an Overall Audit Opinion for the organization.

| Field | Seeded Values | Source | Accessibility Level |
|-------------------------------|---|---|---|
| (Audit Opinion) Conclusion | Effective Deficient Significantly Deficient Materially Weak | Opinions Framework components for the Organization object: * Audit Opinion * Control Environment * Risk Assessment * Control Activities * Information and Communication * Monitoring | Refer to the section: Opinions Framework in Oracle Internal Controls Manager, page 8-29 |

Step 6: Sign Off on the Engagement (if required)

If sign off is required, then the engagement must be submitted and approved before the audit is deemed completed. In this case users will not be able to change the status from "Active" to "Completed."

If sign off is not required, then users can update the status of the engagement to "Completed." The Sign Off Status will remain as "Not Submitted."

Note: For more information on setting up the Sign Off, refer to the section Setup a Sign Off Process, page 8-9.

Engagement Status:

This status is updated as follows:

| Status | Description |
|------------|---|
| Active | All engagements are created with this status |
| Signed Off | When the engagement is complete (and all defined objectives are satisfied), the Engagement Approver updates the engagement to this status |
| Completed | The Signed Off status can be updated to Completed |
| Cancelled | Update to this status if the engagement is cancelled. |

Sign Off Status:

| Status | Description |
|------------------|--|
| Not Submitted | Not Submitted |
| Pending Approval | Once the Engagement is submitted for sign off and prior to approval or rejection |
| Approved | Approved |
| Rejected | Rejected |
| Not Completed | Displayed if there is a problem with the workflow routing. |

Notes on Engagement Execution

Findings in Audit Engagements

You can associate different types of objects (risks, controls, processes, etc.) as well as multiple instances of an object to the same Finding. For example, during the course of an audit engagement, the same non conformity may apply to multiple risks.

The screenshot displays the Oracle Internal Controls Manager interface. The top navigation bar includes 'Home', 'Audit Operations', 'Segregation of Duties', 'Organizations', 'Risk Library', and 'Setup'. The 'Findings' tab is selected. Below the navigation bar, the title bar reads 'Audit Engagement: Americas Sales Audit Q1 2005'. The main content area shows details for the engagement, including Name, Status, Org Unit, Manager, Type, and Risk. The 'Findings' tab is active, displaying a table of findings. The table has columns for Details, Risk, Organization, Process, Open Findings, Evaluation, Evaluation History, and Evaluate. Three findings are listed, each with a 'Findings' icon and a 'Details' icon.

| Details | Risk | Organization | Process | Open Findings | Evaluation | Evaluation History | Evaluate |
|----------|--|------------------|---------|---------------|------------|--------------------|----------|
| Findings | Unauthorized Processing of Supplier Invoices | Vision Computers | ICV 1 | Findings | 0-0 | | Details |
| Findings | Unauthorized Processing of Supplier Invoices | Vision Computers | ICV 1 | Findings | 0-0 | | Details |
| Findings | Unauthorized Processing of Supplier Invoices | Vision Computers | ICV 1 | Findings | 0-0 | | Details |

Note: For more information on creating Findings, refer to Findings in Oracle Internal Controls Manager, page 12-1.

Attachments to Audit Engagements

While executing an audit engagement, it is beneficial to attach all necessary paperwork to the engagement entity. The paperwork can take the form of evidence collected as part of field work as well as contractual documents etc.

You can choose to store the document within the Oracle E-Business suite (Oracle Files) or in an external document management system.

Note: For more information on attaching documents to the Engagements in the application, refer to Attachments in Oracle Internal Controls Manager, page 2-23.

Updates through Business Events

Whenever evaluation, certification, and exception data is created or updated in Oracle Internal Controls Manager, that entry raises a business event. Behind the scenes, multiple event subscribers take note of the change and update the values in all the application's engagement and certification views. The numbers hence reflect the latest data and state of the module.

Note that the application pages display in a disconnected http mode. Hence though the numbers are updated nearly instantaneously in the database tables through event processing, the screen must be refreshed or the page revisited for the changes to display.

Profile AMW: Display option for evaluation and certification numbers

The numbers in the window (for ineffective orgs, processes, etc.) are displayed according to the profile option "AMW: Display option for evaluation and certification numbers." The profile option values are seeded as follows:

- Ineffective (Unmitigated)
- Ineffective (Unmitigated) / Total Evaluated
- Ineffective (Unmitigated) / Total
- Ineffective (Unmitigated) / Total Evaluated / Total
- Percent of ineffective over total (Default).

(Ineffective refers to Organizations, Processes and Controls, Unmitigated refers to Risks)

Opinions Framework in Oracle Internal Controls Manager

There are several different kinds of audit evaluations and certifications that must be entered during an audit conducted using Oracle Internal Controls Manager. For example, routine evaluations are made on process, risk, control, and audit procedure objects. Objects being certified include financial items and statements.

Audit evaluations and certifications are typically made in terms of seeded "opinions." There can be different types of opinions based on the object being evaluated. For example, you enter one type of opinion to record the evaluation of a control object and another type to record the evaluation of an organizational object.

Audit objects in turn have different "component" dimensions and you can enter an evaluation for each of these components. For example, when evaluating a control in a particular process, you can evaluate it in terms of the following:

- Design Effectiveness
- Operating Effectiveness
- An overall Audit Opinion of the control

The Opinions Framework in Oracle Internal Controls Manager provides the following:

1. Seeded opinion values for all components for all objects belonging to the framework. These values correspond to Oracle defined codes.

The following table shows an example of seeded opinion values and their corresponding codes for the Design Effectiveness component of an Organization - Control object.

| Value (user defined) | Code (Oracle defined) |
|-------------------------|-----------------------|
| Deficient | SOMEWHAT_EFFECTIVE |
| Effective | EFFECTIVE |
| Materially Weak | INEFFECTIVE |
| Significantly Deficient | NEARLY_INEFFECTIVE |

2. The ability to create user defined values for opinions that can be selected when making evaluations and certifications. However, the user defined value that you

enter must correspond to an Oracle defined code that is available for the relevant object and opinion.

Note: This correspondence is required because several other features in the application, for example the display of images in the dashboard, are based on these codes values.

The following table shows the details of different objects that are evaluated as a part of the Opinions Framework in Oracle Internal Controls Manager:

| Object | Opinion Type | Component (s) | Seeded Values (for each component) | Notes |
|--|--------------|--|--|--|
| Organization - Audit Procedure - Control | Evaluation | Audit Opinion Design Effectiveness Operating Effectiveness | Effective Significantly Deficient Materially Weak | Discussed in this chapter |
| Organization - Control | Evaluation | Audit Opinion Design Effectiveness Operating Effectiveness | Effective Significantly Deficient Materially Weak | Discussed in this chapter |
| Organization - Process - Risk | Evaluation | Audit Opinion | Mitigated Somewhat Mitigated Somewhat Exposed Fully Exposed | Discussed in this chapter |
| Organization - Process | Evaluation | Audit Opinion | Effective Significantly Deficient Materially Weak | Discussed in this chapter |
| Organization | Evaluation | Audit Opinion Control Environment Risk Assessment Control Activities Information and Communication Monitoring | Effective Significantly Deficient Materially Weak | Discussed in this chapter |
| Key Account | Evaluation | Audit Opinion | Effective Significantly Deficient Materially Weak | See 2. Evaluate and Certify Financial Items. |
| Financial Item | Evaluation | Audit Opinion | Effective Significantly Deficient Materially Weak | See 2. Evaluate and Certify Financial Items. |

Segregation of Duty Constraints

This chapter covers the following topics:

- Introduction
- Responsibilities and Functions in Oracle Applications
- Implementing Segregation of Duties Constraints

Introduction

In order to meet financial objectives, management must ensure that an internal control system is in place that supports the business processes of the organization. In addition, legislation like Sarbanes-Oxley laws in the US require external auditors to render an opinion on the reliability of a firm's internal controls system.

A fundamental principle of a sound internal control system is that there are no users who have access to a group of tasks that are incompatible with each other. At any given time therefore, an individual's job in an enterprise should encompass the rights and responsibilities that come from access to only one task from a set of incompatible tasks.

The segregation of duties control addresses the specific risk that a user may have access to a certain combination of tasks that provide the opportunity for misconduct. Consider the following examples:

- If a user can set up a supplier in an accounts payable system and also authorize an invoice for payment, a risk exists that they can pay themselves with company funds.
- To prevent unauthorized write offs, an individual responsible for inventory accuracy should not be certifying cycle count adjustments.
- Fraud can be perpetrated if systems development staff are involved with live operations.

Segregating duties does not eliminate the risk of collusion between members of staff in different areas, but it does serve as a deterrent. In addition, insulating work in an organization also functions as a safeguard against the possibility of unintentional damage through error. Incompatible tasks are therefore divided among different members of the organization to reduce the scope for error and fraud.

Using Oracle Internal Controls Manager, you now have the ability to identify any combination of tasks in an enterprise as incompatible and report on those occurrences where a single user has access to them.

Once the segregation of duties violations has been identified, auditors can create correction requests to remedy them. These correction requests can be assigned priorities, assigned to different people, and tracked through their lifecycle.

Responsibilities and Functions in Oracle Applications

The Segregation of Duties feature in Oracle Internal Controls Manager is based on access to Responsibilities and Functions in the Oracle E-Business Suite.

Responsibilities

In a typical applications environment, multiple users are assigned a number of Responsibilities in the Oracle E-Business Suite. Responsibilities define application privileges by allowing users access to only those Oracle Applications functions and data appropriate to their roles in the organization. Each responsibility allows access to the following items (among others):

- A specific application or applications, such as Oracle General Ledger or Oracle Planning as well as a Set of Books.
- A restricted list of windows that a user can navigate to; for example, a responsibility may allow certain Oracle Planning users to enter forecast items, but not enter master demand schedule items.
- A restricted list of functions a user can perform. For example, two responsibilities may have access to the same window, but one responsibility's window may have additional function buttons that the other responsibility's window does not have.

Functions

Functions are a security feature in Oracle Applications that are used to control access to specific application features. Each function typically corresponds to an application feature like a page, button, tab, or menu.

Functions translate into duties/tasks in the modules and are therefore equivalent to the actions that users can perform. Only if a particular function is included in a user's responsibility will that individual be able to access the feature and execute the task. Oracle E-Business Suite applications come pre-seeded with a large number of relevant functions. By treating form functions as tasks, the Segregation of Duties feature integrates seamlessly with the Oracle E-Business Suite security model.

Manual Functions and Functions in External Applications

You can also create your own functions and select them in Oracle Internal Controls Manager. This makes the Segregation of Duties functionality also extendable to tasks performed manually. For example, if one wants to specify that the night security guard should not have access to the master keys, then two functions can be created for each of these tasks and subsequently assigned to users.

Tasks performed in other ERP or legacy systems can also be handled in this fashion. If you use functions that originate in third party applications, then you will need to set the profile options shown below to map the users, responsibilities, functions, etc. in those systems to Oracle Internal Controls Manager. The external entities will then be recognized by the Oracle application.

The following table lists the profile options that must be seeded if Oracle E-Business functions are not used.

Note: For detailed information on the use of functions, also refer to Managing Oracle Applications Security, in the *Oracle Applications System Administrator's Guide*.

| Profile Option | Description | Required Columns | Default Value (Oracle) |
|---|---|---|------------------------|
| AMW: Table for Users | This table/view stores information about application users. Each row includes the user's username (what a user types in at the sign-on screen) | USER_ID USER_NAME PERSON_PARTY_ID START_DATE END_DATE | FND_USER |
| AMW: Table for User Responsibilities | This table/view stores information about the responsibilities assigned to an application user. Each row includes values that identify the user and the responsibility. Each row also contains a start date and end date for that responsibility assignment. You need one row for each responsibility assigned to each application user. Oracle Application Object Library uses this information to determine which forms and menus a user can access. | USER_ID RESPONSIBILITY_ID RESPONSIBILITY_APPLICATION_ID START_DATE END_DATE CREATED_BY | FND_USER_RESP_GROUP PS |
| AMW: Table for Responsibilities | This table/view stores information about responsibilities. Each row includes the application it belongs to and values that identify the main menu that the responsibility uses. You need one row for each responsibility at your site. | RESPONSIBILITY_ID RESPONSIBILITY_KEY APPLICATION_ID MENU_ID START_DATE END_DATE | FND_RES_PONSIBILITY |
| AMW: View for Responsibility Name | This is a view of the above table. | RESPONSIBILITY_ID RESPONSIBILITY_KEY APPLICATION_ID MENU_ID START_DATE END_DATE RESPONSIBILITY_NAME | FND_RES_PONSIBILITY_VL |

| Profile Option | Description | Required Columns | Default Value (Oracle) |
|---|---|--|------------------------|
| AMW: Table for Exclusion Function Rules | <p>This table/view stores security exclusion rules for function security menus. Security exclusion rules are lists of functions and menus inaccessible to a particular responsibility. Each row includes an action identifier whose value is dependent on the rule type.</p> <p>In the pseudo code below, F=Function and M=Menu. (ACTION_ID=FUNCTION_ID from AMW_FORM_FUNCTIONS if RULE_TYPE='F' or ACTION_ID=MENU_ID AMW_MENUS if RULE_TYPE='M')</p> | RESPONSIBILITY_ID ACTION_ID RULE_TYPE APPLICATION_ID | FND_RESP_FUNCTIONS |
| AMW: View for Function Name | This table/view stores information about function grouping in forms. Each row includes a function identifier, the function name, and the application identifier. You need one row for each function. | FUNCTION_ID FUNCTION_NAME APPLICATION_ID TYPE USER_FUNCTION_NAME MAINTENANCE_MODE_SUPPORT CONTEXT_DEPENDENCE | FND_FORM_FUNCTIONS_VL |
| AMW: Table for Menus | This table/view lists the menus that appear in the Navigate Window, as determined by the System Administrator when defining responsibilities for function security. Each row includes a menu name and identifier. You need one row for each menu (and each submenu) in each application. | MENU_ID TYPE MENU_NAME | FND_MENUS |
| AMW: View for Menu Names | This is a view of the above table. | MENU_ID TYPE MENU_NAME USER_MENU_NAME | FND_MENUS_VL |

| Profile Option | Description | Required Columns | Default Value (Oracle) |
|--|---|---|-----------------------------|
| AMW:Table for Menu Entries | This table/view stores information about individual entries in the table specified by the profile option "AMW:Table for Menus." Each row includes an ID number that identifies the menu to which the entry belongs, a sequence number that determines the order in which the entry appears on the menu (relative to other choices on the same menu), the submenu and/or function attached to the entry. You need one row for each entry (menu choice) in each navigate window menu. | MENU_ID ENTRY_SEQUENCE SUB_MENU_ID FUNCTION_ID GRANT_FLAG | FND_MENU_ENTRIES |
| AMW:Flat view for Menu Function Relation | This table compiles the information from the table specified by the profile option "AMW:Table for Menu Entries." This facilitates runtime lookups of which functions are on which menus. It collapses the hierarchy in the above table into a flat format. This does not take exclusions into account. | MENU_ID FUNCTION_ID GRANT_FLAG | FND_COMPILED_MENU_FUNCTIONS |

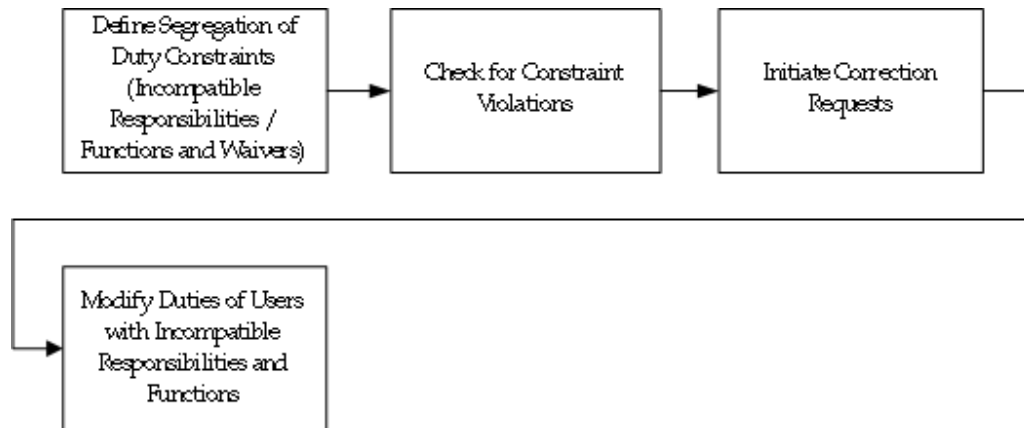
Implementing Segregation of Duties Constraints

Oracle Internal Controls Manager can be used very effectively to check whether the users in the enterprise have access to responsibilities and functions that are incompatible with each other. The application facilitates the proactive monitoring and reporting of incompatible tasks.

Note: Users are not restricted to employees in the Oracle HR system. The application recognizes any individual defined in Oracle Applications as a user (all those listed in the FND_USER table).

You now have the ability to identify any specific combination of incompatible responsibilities or functions in an organization as a constraint. The application can then report occurrences where an individual possesses access to two or more of these incompatible tasks and thereby violates the constraint. When a constraint violation is found, you can initiate a correction request for management to take action by modifying the duties of those users with incompatible tasks.

The following diagram displays the steps to implement segregation of duties constraints in Oracle Internal Controls Manager.



The steps to create segregation of duties constraints and rectify violations are listed below:

1. Define Segregation of Duty Constraints
2. Check for Constraint Violations
3. Initiate Correction Requests
4. Modify Duties of Users with Incompatible functions.

These steps are described in the sections below with an illustrative example.

1. Define Segregation of Duty Constraints

Constraints are created by setting up either

- Two or more responsibilities or
- Two or more functions

as incompatible with each other. Your first task is therefore to define a seeded registry of constraints i.e. incompatible jobs and duties that should not be performed by the same user.

For the purposes of this example, assume that we have just one set of conflicting duties - the organization does not want users who can create purchase orders to be able to also enter invoices and vice versa.

Note: The incompatible responsibilities and functions can span application modules - for example responsibilities or functions in Oracle Purchasing and Oracle Payables can be setup as incompatible..

| Topic | Navigation Path |
|--|---|
| Create Segregation of Duty Constraints | Using the Internal Auditor (or equivalent) responsibility, navigate to the Segregation of Duties tab and then the Constraints subtab. |

Define Segregation of Duty Constraints in the following way:

- a. Enter the basic attributes of the constraint

- b. Setup two or more incompatible functions or responsibilities
- c. Optionally setup Responsibility and/or User waivers

a. Enter the basic attributes of the constraint.

The constraint name in this example is "PO-Invoice SOD."

The following table provides further information on select fields in the Segregation of Duties Constraint page.

| Field | Details |
|-----------------------------------|--|
| Risk | The risk that arises when this constraint is violated. The list of values shows all risks that have been seeded in the Risk Controls library. |
| Violation Definition radio button | <p>A violation will exist in any one of the following cases:</p> <p>"User possesses all functions/responsibilities from the set of incompatible functions/responsibilities"</p> <p>"User possesses any two functions/responsibilities from the set of incompatible functions/responsibilities."</p> <p>The actual set of incompatible functions and responsibilities is defined in the subsequent window - Step b. below</p> |

b. Setup two or more incompatible functions or responsibilities

Setup of incompatible responsibilities: If the constraint involves responsibilities, then all existing responsibilities in the registered applications of the Oracle E-Business Suite are available. Had responsibilities been used in our example, then typical Purchasing and Payable responsibilities would be made incompatible with each other.

- Subfunction - Subfunctions added to menus (without prompts) to provide security functionality for forms or other functions.
- JSP - Functions used for some products in the Oracle Self-Service Web Applications suite. These are typically JSP functions.
- WWW - Functions used for some products in the Oracle Self-Service Web Applications suite. These are typically PL/SQL functions.

Note: For more information on Function Type, refer to the *Oracle Applications Developer's Guide*.

You will need to know the Type and/or Name of relevant functions to isolate them when defining constraints.

In our example, as both the entering of invoices and creation of purchase orders correspond to forms within Oracle Payables and Oracle Purchasing, both Types of functions in the example will correspond to "Form."

c. Optionally setup Responsibility and/or User Waivers

You may optionally set up exceptions to the constraint in the form of "waivers." Responsibility and User Waivers specify one or more responsibilities and users for which the constraint (that is being setup) will not apply. As an example, a Payables Super User may be exempted from the company wide rule that individuals who have access to purchase orders can enter invoices as well.

The two types of waivers are distinct i.e. the constraint is not deemed violated by individuals listed under User Waivers nor by those who have access to the responsibilities listed under Responsibility waivers. Note that waivers can be restricted to a particular date range by entering the End Date for the waiver.

Note: Only user waivers can be setup for responsibility constraints.

Create Constraint Cancel Back Step 3 of 3 Finish

Responsibility Waivers

| Responsibility Key | Responsibility Name | Start Date | End Date |
|-------------------------|--|-------------|----------|
| PAYABLES_VISION_PROCESS | Payables Super User (Process Operations) | 29-Mar-2005 | |

User Waivers

| User Name | Employee Name | E-mail Address | Start Date | End Date |
|-----------|------------------|----------------|-------------|----------|
| JABBOTT | Abbott, Mr. John | | 29-Mar-2005 | |

Importing Segregation of Duty Constraints

Instead of manually entering the segregation of duty constraints, you can now use Web ADI to import constraints into the application. Web ADI provides many advantages including the use of a native spreadsheet interface.

| Topic | Navigation Path |
|--|---|
| Import Segregation of Duty Constraints | Using an Internal Auditor (or equivalent) responsibility, click the Segregation of Duties tab and then the Import subtab. |

Use the "Import Constraints" hyperlink to import constraint details into the application. Oracle Internal Controls Manager first requires that you select user settings like the viewer (Excel 1997/2000). The spreadsheet is then displayed and you can enter/copy values into these cells. Finally select Oracle - Upload from the menu bar to begin the import process.

The following table lists the fields in the import spreadsheet:

| Field Name | Mandatory | Validation |
|-------------------------------|-----------|--|
| Constraint Name | Yes | NA |
| Start Date | Yes | MM-DD-YYYY |
| Violation Definition | Yes | Function: All - User possessing all functions from the set of incompatible functions Function: Mutually Exclusive - User possessing any two functions from the set of incompatible functions Responsibility: All - User possessing all responsibilities from the set of incompatible responsibilities Responsibility: Mutually Exclusive - User possessing any two responsibilities from the set of incompatible responsibilities |
| Description | No | NA |
| End Date | No | MM-DD-YYYY |
| Risk Name | No | All valid risk names in the OICM Risk Library |
| Incompatible Functions | No | All existing functions in the registered applications of the Oracle E-Business Suite |
| Incompatible Responsibilities | No | All existing responsibilities in the registered applications of the Oracle E-Business Suite |

Note: The import spreadsheet cannot be used to import constraint waivers. Once Segregation of Duty Constraints are imported into the application, query them up and append any Responsibility or User waivers as necessary.

Web ADI uploads the data from the spreadsheet into the AMW_CONSTRAINT_INTERFACE interface table. A concurrent program then uploads the data from the interface table to the base tables. Any errors that occur during the import process are flagged as errors with appropriate error messages.

If set to "Yes," the profile option AMW: Constraints - Delete after Import will delete controls from the interface table after their successful import via WEBADI.

For Web ADI to work with Excel 2002 (XP), perform the following three steps:

1. Open Excel 2002
2. Go to Tools -> Macro -> Security -> Trusted Sources
3. Check the "Trust access to Visual Basic Project"

2. Check for Segregation of Duties Constraint Violations

Now launch the concurrent process "Check Violation for Constraints" that checks for incompatible functions belonging to the same user.

| Topic | Navigation Path |
|--|--|
| Launch check for segregation of duties constraint violations | Using the Internal Auditor (or equivalent) responsibility, navigate to the Segregation of Duties tab and then the Constraint Violations subtab. Click the "Check for Violations" button |

Note the following options when running this process:

- You can run the concurrent program to check for "All" or for one to four specific constraints.

The screenshot shows the 'Schedule Request: Parameters' window. At the top, there's a navigation bar with tabs: Home, Audit Operations, Segregation of Duties (selected), Organizations, Risk Library, and Setup. Below this is a subtab bar with: Constraint Violations (selected), User Violations, Requests, Constraints, and Import. A progress bar shows five steps: Name, Parameters (current), Schedule, Notifications, and Review. The main content area is titled 'Schedule Request: Parameters' and includes a 'Cancel' button, 'Back' button, 'Step 2 of 5', and 'Next' button. Below this, it says '* Indicates required field'. The 'Program Name' is 'Check Violation for Constraints' and the 'Request Name' is 'Check for PO-Invoice SOD Violations'. There's a section for '* Check Violation for All Constraints' with a dropdown menu set to 'No'. Below that are four 'Constraint Name' input fields; the first one contains 'PO-Invoice SOD Violations'. To the right of these fields are four small blue icons representing a printer or notification.

- You can set the program to repeat automatically on a predefined schedule. A recurring schedule enables the proactive monitoring and reporting of incompatible functions among users of your applications.
- You can send a notification to one or more individuals. The notification informs the user that the process was submitted along with the status of the submission.
- As the concurrent process "Check Violation for Constraints" can run for several minutes in a large installation, the application provides the ability to monitor the process within the Segregation of Duties > Requests subtab. You therefore do not need to use a System Administrator responsibility to view the status of these requests.

Review Segregation of Duties Violations

When the concurrent process completes, Oracle Internal Controls Manager provides a detailed roster of constraint violations. You can search for these violations by constraint name in the Segregation of Duties > Constraint Violations window.

The screenshot shows the Oracle Internal Controls Manager interface. At the top, there is a navigation bar with tabs: Home, Audit Operations, Segregation of Duties (selected), Organizations, Risk Library, and Setup. Below this is a sub-navigation bar with links: Constraint Violations (selected), User Violations, Requests, Constraints, and Import. The main title is "Segregation Of Duties Constraint Violations". On the right, there is a "Save Search" button and a "Shortcuts" section with links to Constraint Violations, User Violations, and Monitor Requests. Below this is a "Simple Search" section with a note: "Please note that the search is case insensitive." and an "Advanced Search" button. A search input field contains "po" with "Go" and "Clear" buttons. Below the search is a "Check For Violations" button and a table with the following data:

| Constraint Name | Request Id | Time Checked | Requested By | Num of Violating Users | Violation Status | Correction Requests | XML Report |
|---------------------------|------------|----------------------|--------------------|------------------------|------------------|---------------------|------------|
| PO-Invoice SOD Violations | 2762107 | 30-Mar-2005 07:50:35 | Dorobo, Mr. Martin | 353 | Open | | |

Note that a history with respect to running the "Check Violation for Constraints" process is maintained in this window. Hence if corrective action is being taken (described in the next section), a particular constraint should show a reduction in the "Number of violating users" over time.

Violation Status: The following table provides details on this column.

| Status | Details |
|----------------|---|
| Closed | If the number of violating users is zero |
| Not Applicable | If changes were made to the constraint since the last run of the Check Violations for Constraints program |
| Open | If the number of violating users is greater than zero |

You may drill down to find the details of each user violating this particular constraint along with a list of incompatible job functions held by that user. The Waived Users subtab lists all users who are setup as exempted from violating the exemption.

[Home](#)
[Audit Operations](#)
[Segregation of Duties](#)
[Organizations](#)
[Risk Library](#)
[Setup](#)

[Constraint Violations](#)
[User Violations](#)
[Requests](#)
[Constraints](#)
[Import](#)

Segregation of Duties: Constraint Violations >

Constraint Violation Details

| | | | |
|-----------------|---------------------------|----------------------|--|
| Constraint Name | PO-Invoice SOD Violations | Violation Status | Open |
| Date Checked | 30-Mar-2005 | Violation Definition | User possessing any two functions from the set of incompatible functions |

[Users](#)
[Waived Users](#)
[Correction Requests](#)

Search

User Name

Previous
1-10
Next 10

| Details | User Name ▲ | Employee Name | Manager Name |
|---------|-------------|------------------|------------------|
| ▶ Show | ABOASE | Boase, Alex | Bart, Lou |
| ▼ Hide | ADB | Brady, Ms. Kathy | Brown, Ms. Casey |

| Violation Entries | | | | |
|-------------------|--------------------|---|-------------------|-----------------|
| Function | Submenu | Responsibility | Access Given Date | Access Given By |
| Purchase Orders | Purchase Orders: | Purchasing, Vision Banking | 01-Jan-1000 | |
| Invoices | AZN_PR_PROCUREMENT | Purchasing, Vision Banking | 01-Jan-1000 | |
| Invoices | AZN_PR_PAYABLES | Payables, Vision Banking | 01-Jan-1000 | |
| Invoices | AZN_PR_PAYABLES | General Ledger, Vision Banking, Manager | 01-Jan-1000 | |

| | | | |
|--------|----------|-------------------|-------------------------|
| ▶ Show | AHOBBS | Hobbs, Andie | Allen, Bertie |
| ▶ Show | AJOHNSON | Johnson, Ms. Alex | Horton, Ms. Connor Esq. |

User Violations: Note that you can also search for all constraints that a particular user is violating in the Segregation of Duties > User Violations window.

3. Initiate Correction Requests (and Subsequently Modify User Duties)

Once a segregation of duties violation is discovered, you can initiate a Correction Request to correct the violation and therefore mitigate the risk from users having access to incompatible tasks in the organization. In our example, this will comprise the removal of either the Purchasing or Invoice functions from the responsibility of users who have access to both.

Correction Requests may be viewed primarily as a platform where the request for corrective action is initiated and tracked. The initiation of such a request does not automatically remove access to responsibilities and functions from violating users. Ultimately a system administrator (or person with an equivalent responsibility) must modify the responsibilities of those users so that no individual has access to conflicting functions and responsibilities.

Note that Correction Requests can be assigned to a particular user and then tracked in the application.

Note: For more information on setting up Correction Requests, refer to Correction Requests in Oracle Internal Controls Manager, page 12-15.

Step 1: Create the Request

| Topic | Navigation Path |
|-----------------------------|---|
| Create a correction request | <p>Using the Internal Auditor (or equivalent) responsibility, click the Segregation of Duties tab and then the Constraint Violations subtab. The window shows a detailed listing of violations.</p> <p>Click the Correction Requests icon for a particular constraint violation and then the Create button OR</p> <p>Drilldown into a violation, click the Correction Requests hyperlink and then the Create button</p> |

Home Audit Operations **Segregation of Duties** Organizations Risk Library Setup

Constraint Violations | User Violations | Requests | Constraints | Import

Segregation of Duties: Constraint Violations > Constraint Violation Details >

Create Correction Request

* Indicates required field Cancel Save for Later (Q) Submit

Correction Request Type **DutyViolat**

Correction Request Number **VIOLATION2**

* Correction Request Name Initiate changes for PO-Invoice SOD Violations


Description



Remove access to the Purchase Order creation function for the following users:
Alan Aron
Alex Boase


Remove access to the Invoice Entry function for the following user:
Kathy Brady

Constraint Name **PO-Invoice SOD Violations**

Additional Information Dependencies Workflow Approval Attached Documents

* Assigned To Martin Dorobo  Requestor Martin Dorobo

Priority High  Need By Date 
(example: 30-Mar-2005 19:45:00)

Reason Fraud 

The following table provides further information on select fields used in the Create Correction Requests window.

| Field | Details |
|----------------------------------|--|
| Correction Request Number / Name | User defined number and name to identify and track the request to correct the constraint violation |
| Priority | User defined Priority rating - Seeded using Issues Management functionality (See Chapter 12) |
| Reason | User defined Reason - Seeded using Issues Management functionality (See Chapter 12) |

Note: You can also attach documents to the correction request for further clarification.

Correction Request Report: Instead of choosing to create a Correction Request (using the Create button), you can create an ad hoc report for details on the correction request.

| Topic | Navigation Path |
|------------------------------------|--|
| Create a Correction Request Report | Using the Internal Auditor (or equivalent) responsibility, click the Segregation of Duties tab and then the Constraint Violations subtab. The window shows a detailed listing of violations. Click the Correction Requests icon for a particular constraint violation and then the View Reports button. Finally, click the Create Reports button. |

Note that before you can view the report, Oracle Internal Controls Manager requires you to choose "Report Criteria" and a "Results Format" for the production of the report.

The criteria and results are based on fields like Request Number, Assigned To, Created By, Requested By, Creation Date, Need By Date, etc. Results are displayed in four sections:

- People
- Attachments
- Approval
- Action Log

Step 2: Track the Request

| Topic | Navigation Path |
|------------------------------|--|
| Track the correction request | Using the Internal Auditor (or equivalent) responsibility, click the Segregation of Duties tab and then the Constraint Violations subtab. The window shows a detailed listing of violations. Click the Correction Requests icon and then drilldown into the relevant request (by clicking on the request number). |

The Correction Requests Summary window acts as a bulletin board where you can view details of the request as well as changes in status over time.

There are several possible actions that you can take like Change priority, Post Comments, Cancel, Promote, Put on Hold, Re-assign, Update corrections and Request Comments. Oracle Internal Controls Manager maintains an exhaustive history of the correction request in this window.

Process and Organization Certification

This chapter covers the following topics:

- Introduction
- Overview of Process / Organization Certification
- Corporate Processes vs. Organization (Local) Processes
- Implementing Process / Org Certification in Oracle Internal Controls Manager
- Process / Org Certification: Global Operations Controller
- Process / Org Certification: Business Process Owner
- Certification Notes
- Creating and Resolving Issues in Certification

Introduction

Corporate management systems typically imply the existence of processes that are employed to implement the objectives of management. For these management systems to be effective, it is critical that the business processes supporting them are regarded as reliable.

In addition, the implications of complying with legislation like the Sarbanes-Oxley Act in the USA, provides further impetus to ascertaining the adequacy of internal controls in the execution of business processes. Audited business processes are a critical factor in the overall monitoring scheme of a firm. The issuance of certification attests to the process and/or organization being in compliance with standards as required by compliance legislation.

This chapter provides all the information you need to know to certify your business processes and organizations (orgs) using Oracle Internal Controls Manager.

Overview of Process / Organization Certification

The COSO body defines the internal control system itself as a "process." It is imperative that the process based nature of internal controls be recognized and incorporated into audits of the control system. Companies therefore need to establish an ongoing monitoring of business processes while evaluating and improving their effectiveness.

One way of accomplishing this objective is through the periodic certification of processes and organizations in the enterprise. Certification requires process owners to provide assurance that their organization's processes are in compliance with the standard(s)

utilized as the basis of its management system. It includes a series of rigorous audits and other activities to provide assurance that the organization's management system is adequate and effective.

Successful completion of an audit and any related follow-up activities which may be required results in the process being "certified." The certification attests to the process meeting the requirements of the applicable standard.

External auditors seek objective evidence of such a system being established and effectively implemented before they can attest to the accuracy of financial statements. Certified business processes also provide comfort to CFOs, CEOs, and audit committees as they attest to the adequacy of internal controls and the accuracy of financial results.

Ongoing requirement

As a certification is considered valid for a particular time frame, processes must still be audited on a periodic basis to ensure that they continue to remain effective. This requirement leading to continual re-certification lends credibility to the entire corporate management and control system. Depending on the requirements, re-certification is typically conducted at intervals of three months for the significant processes and greater for less important ones.

Input from the Audit Engagement

Though some processes are audited infrequently or not at all, the majority of significant business processes in the entity are subject to a periodic audit. As noted in an earlier chapter, the audit engagement represents a compilation of audit assignments for the entity and is typically associated with the audit of a process. The audit engagement gathers evidence indicating whether the process is fully functional and meets the requirements of applicable standard(s).

Major nonconformities can be identified during the audit and in such cases a certification cannot be issued until these are effectively addressed and remedied. At a minimum, these "findings" must be taken into account prior to certification. Post audit "issues" that arise during the actual certification must also be recorded. The Auditor can make a recommendation for certification upon closure of all identified nonconformities i.e. Findings and Issues.

Note: For more information, refer to Creating and Resolving Issues in Certification, page 10-20.

The results from an audit of the process (through an audit engagement) provide an independent perspective to process owners and serve as an aid to certification.

Input from Assessments

Process owners are also expected to utilize their day-to-day working knowledge of processes to certify them. To this end, they can conduct Assessments of their processes and organizations with respect to the organizations internal control structure and compliance.

The results of the Assessment provides further evidence indicating whether the process meets the requirements of applicable standard(s) and can be certified.

Process Certifications and Financial Statements

Process certification in Oracle Internal Controls Manager "flows" into a signing officer's view on line items in financial statements. The signing officer can drilldown into the process that supports a particular financial line item. The audit evaluation along with process certifications provides two independent views of those processes and aids in the certifying of financial statements.

Corporate Processes vs. Organization (Local) Processes

In addition to the processes executed in the organizations (auditable units) of your firm, Oracle Internal Controls Manager also allows you to create "Corporate" processes.

Corporate processes have a global orientation and can be thought of as being executed by a central governing body across all organizations in the enterprise. As opposed to corporate processes, regular organization (local) processes are processes executed within a specific organization in the enterprise. Local processes include standard processes as well as their variants in the organization.

Note: For more information on variant processes, refer to Process Variation Management, page 3-12.

Corporate processes include both of the following:

- Consolidation of core processes in various organizations such as order-to-cash under enterprise level managers.

Consider the following example to understand the functionality of such a corporate process in Oracle Internal Controls Manager. Assume a corporate process "Order-to-cash" is created in the enterprise. As noted above, this process is considered to be a consolidation of the order-to-cash processes in the various organizations of the enterprise.

By drilling into this process, Oracle Internal Controls Manager displays a detailed listing of all the local processes (having the same name as the corporate process) in all organizations. It is important to note that the list includes all standard "Order-to-cash" processes as well as their variants.

You can therefore obtain a comprehensive and consolidated view of this process across the enterprise and use that input in the certification of the corporate process.

- Processes executed solely for the benefit of the enterprise and not any specific organization. Oracle Internal Controls Manager does not provide any specific functionality for these types of corporate processes and they display the functionality of a regular process.

To create a corporate process

Corporate processes are enabled in the application by the creation of an organization representing the enterprise that executes these processes i.e. to create a corporate process, you first need to create a corporate organization.

The corporate organization is an organization (auditable unit) in Oracle Internal Controls Manager that is seeded in the profile option AMW: Headquarters. This global org should also be the root org of the organization hierarchy.

Note: For more information on creating organizations in Oracle Internal Controls Manager, see Organizations in Oracle Internal Controls Manager.

Any process that is attached to a corporate organization is by definition a corporate process. The corporate process has all the attributes of a regular process including a designated owner. Hence, if corporate processes are present and executed by the enterprise, they are automatically included in the scope of process certifications as well. The corporate process will be listed in certification windows along with other processes that belong to the designated process owner.

Note: You can easily distinguish a corporate process in Oracle Internal Controls Manager certification windows by its globe icon.

Implementing Process / Org Certification in Oracle Internal Controls Manager

Oracle Internal Controls Manager is pre-seeded with two responsibilities that are used to implement process certifications, the Global Operations Controller and the Business Process Owner.

The application distinguishes between the two as follows:

- The Global Operations Controller creates process certification requests. These requests are sent out in the form of notifications to process owners to do what is necessary to certify their business processes. This responsibility is analogous to a process super user and has the ability to view and update the certification statuses of all processes in the enterprise.
- The individual logged in as a Business Process Owner can view only those processes that they own (along with associated sub processes) as well as processes within organizations that list them as the organization owner.

Note: For more information, refer to Roles and Privileges, page 15-1 and Function Security, page 16-1 in Oracle Internal Controls Manager.

Process owners can certify these processes thereby indicating their satisfaction with the adequacy and effectiveness of their internal controls. Certification takes the form of "Certified" or "Certified with Issues." This nomenclature can be changed using the Opinions framework.

Note: For detailed information on the Opinions framework, refer to Opinions Framework in Oracle Internal Controls Manager, page 8-29.

As noted in an earlier section, audit evaluations from engagements that have audited a process serve as one of the inputs used by process owners in the evaluation of that process.

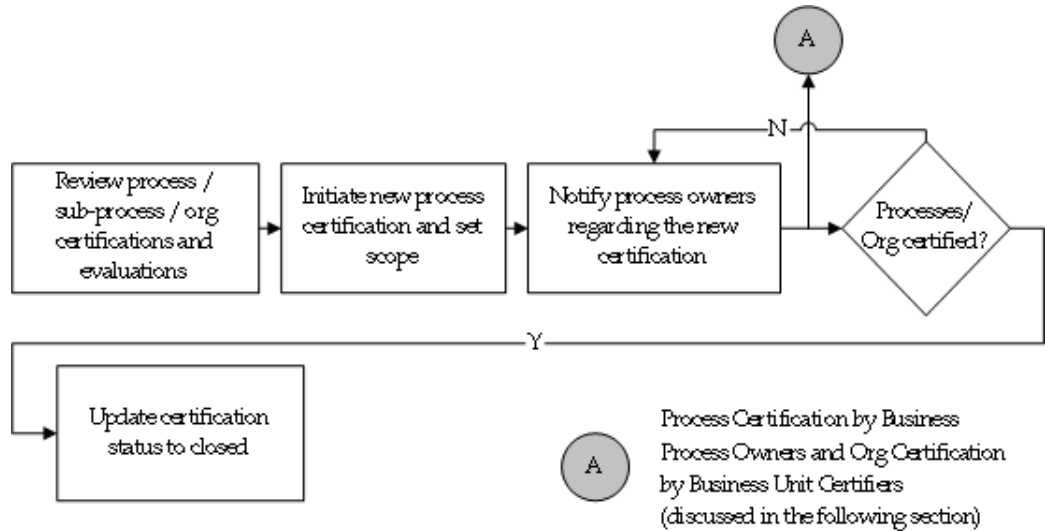
Both Global Operations Controllers and Process Owners have access to the audit evaluation of processes. The following audit engagement results can be used by business process owners:

1. Unmitigated risks

2. Ineffective controls
3. Findings

Process / Org Certification: Global Operations Controller

The following diagram shows a high level view of the tasks performed by a Global Operations Controller to certify the firm's business processes:



1. Review Certifications and their Current Evaluations

The Global Operations Controller responsibility provides a high level view of the certification effort in all processes and in all organizations in the enterprise. Before initiating any new reviews, review the current status of process compliance as shown below.

| Topic | Navigation Path | Oracle Internal Controls Manager Window |
|--|--|---|
| Global Operations Controller view of process certification | Using the Global Operations Controller responsibility, click the Business Process tab and then the Certifications subtab | Certifications |

Home

Business Processes

Segregation of Duties

Organizations

Risk Library

Settings

Certifications

Assessments

Remediation

Findings

Issues

Certifications

Views

View: All

Go

Personalize

Simple Search

Create

| Certification Name | Certification Type | Certification Owner | Quarter | Year | Certification Status | Creation Date | Target Completion Date | Organizations Pending Process Certification | Organizations Pending Certification |
|---|--------------------|---------------------|---------|------|----------------------|---------------|------------------------|---|-------------------------------------|
| OS Business Process Certification | SOX 404 | Fraser, Mr. Landon | Q4 | 2005 | Draft | 21-Mar-2005 | 31-Mar-2005 | 2 / 3 | 0 / 3 |
| Q1 2006 Certification | SOX 404 | Fraser, Mr. Landon | Q1 | 2006 | Draft | 15-Mar-2005 | 15-Mar-2006 | 11 / 11 | 11 / 11 |
| Q2 2006 Certification | SOX 404 | Fraser, Mr. Landon | Q2 | 2006 | Draft | 09-Mar-2005 | 31-Mar-2006 | 6 / 15 | 0 / 19 |
| Q3 2006 Certification | SOX 404 | Fraser, Mr. Landon | Q3 | 2006 | Draft | 10-Feb-2005 | 31-May-2006 | 2 / 0 | 2 / 0 |
| Q4 2004 Certification | SOX 404 | Fraser, Mr. Landon | Q4 | 2004 | Active | 13-Dec-2004 | 31-Dec-2004 | 9 / 8 | 8 / 8 |
| Q1 2004 Certification | SOX 404 | Fraser, Mr. Landon | Q1 | 2004 | Active | 04-Dec-2004 | 31-Dec-2004 | 1 / 9 | 9 / 9 |

This window lists all certifications that have been initiated in the enterprise. A certification is a container, analogous to an engagement, and represents a compilation of processes undergoing certification. You can drill into a certification (by clicking on the certification hyperlink) to view the processes under it.

A process certification includes a set of processes as determined by its scope. However, an individual other than the Global Operations Controller, will be able to view only those processes (and associated sub processes):

- that list them as the designated process owner
- within organizations that lists them as the organization owner

The "Organizations Pending Process Certification" column reflects the number of organizations in the enterprise that have at least one "first level" process being executed in them that is uncertified. First level processes are the processes immediately under the "All Processes" node.

In the following example, P1, P2, and P3 are first level processes. Assume that Process P1 and Process P2 are being executed in Organizations A and B and Process P3 is being executed in Organization C. Further, P1 and P2 are certified in Organization A while P2 is uncertified in Organization B. P3 in Org C is also uncertified.

| Organization | Processes in the Org | Certified |
|--------------|----------------------|-----------|
| A | P1, P2 | P1, P2 |
| B | P1, P2 | P1 |
| C | P3 | None |

For the scenario described above, the Organizations Pending Process Certification column displays "2/3" as both Organizations B and C have at least one first level process in them that is uncertified.

The "Organizations Pending Certification" column reflects the number of organizations in the enterprise that are uncertified. For example 1/3 in this case reflects 3 orgs in scope of which 1 is uncertified.

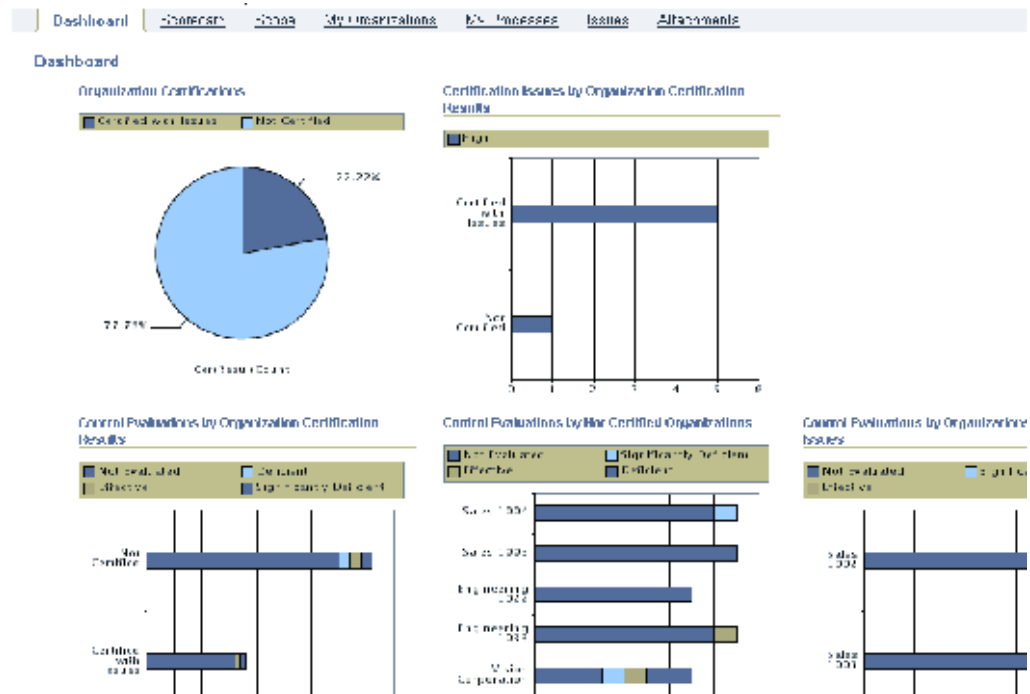
Note: The profile option setting "AMW: Display option for evaluation and certification numbers" is not valid for these two columns
 - Organizations pending process certification and Organizations pending certification.

For more information on this profile option, refer to the Certification Notes, page 10-19 later in this chapter.

Click on a certifications hyperlink to view the following:

Dashboard

The Dashboard tab view is restricted to those logging in with Global Operations Controllers responsibility and provides a summary view of audit evaluation results and certifications across all organizations in the enterprise.



The Dashboard has seven sections as follows:

- Organization Certifications
- Certification Issues by Organization Certification Results
- Control Evaluations by Organization Certification Results
- Control Evaluations by Not Certified Organizations
- Control Evaluations by Organizations Certified with Issues
- Open Findings - Top 5 Organizations

- Open Remediations - Top 5 Organizations

Scorecard

This window also displays a comprehensive view of the state of the certification to Global Operation Controllers in three sections as follows:

- Changes to Processes in Scope (since the beginning of the certification period)
Displays a summary view of any additions in risks or mitigating controls (for the processes in scope) that have been created in the enterprise since the start of the certification period.
- Corporate Processes and Organizations Processes
Lists the number of processes that are uncertified or certified with issues in the enterprise.
Note: For more details, see Corporate Processes vs. Organization (Local) Processes.
- Audit Evaluation
Displays the number of processes (Corporate and Organization) with "Ineffective Controls" and "Unmitigated Risks." These numbers are from the most recent evaluations of the respective processes across audit engagements.

Scope

Displays a list of all entities in the scope of the current certification. You can now view the certification scope through a hierarchical filter. Three hierarchy views are available:

1. Custom Hierarchy. This is the hierarchy of organizations as defined in the Oracle HR module and entered in the "AMW: Org Security Hierarchy" profile option.
2. Legal Hierarchy. This is the hierarchy of subsidiaries (companies) in the Subsidiary Value Set. The value set name must be entered in the "AMW: Subsidiary Value Set for Audit Units" profile option.
3. Management Hierarchy. This is the hierarchy of LOB's in the LOB Value Set. The value set name must be entered in the "AMW: LOB Value set for Audit Units" profile option.

Oracle Internal Controls Manager

Home Business Processes Segregation of Duties Organizations

Certifications Assessments Remediation Findings Issues

Business Processes, Certifications >

Certification: Q1 2004 Certification

Auto Reminder (in days): Description: Certification for Q1 2004

Dashboard Scope My Organizations My Processes Issues Attachments

View: Legal Hierarchy

Expand All Collapse All

| Locals | Organization | Type | Location | Manage Included Processes | Remove |
|--------|--------------------|------------------------|-------------------|---------------------------|--------|
| | Root Node | | | | |
| | US Operations | | | | |
| | Vendor Corporation | Corporate Headquarters | 4B- New York | | |
| | Engineering 1222 | Cost Centre | VI- New York City | | |
| | Engineering 1700 | Cost Centre | VI- New York City | | |
| | Sales 1001 | Cost Centre | VI- New York City | | |
| | Sales 1002 | Cost Centre | VI- New York City | | |
| | Canada Operations | | | | |

Note: For detailed information on creating certification scope, refer to Set the Scope of the Certification, page 10-13.

My Organizations

This window provides a comprehensive "dashboard" view of all organizations along with their associated evaluations and certifications in the enterprise. As noted earlier, the Global Operations Controller views all organizations in the enterprise while others view only the organizations and LOBs according to their roles and privileges.

Note: For more details on access rights in the application, refer to Roles and Privileges, page 15-1 and Function Security, page 16-1 in Oracle Internal Controls Manager.

You may drill into an organization to get a detailed view of the processes (along with associated risks and controls) being executed in that organization.

are from the most recent evaluation of this organization as conducted through an audit engagement. This evaluation is typically done by the firm's internal audit staff and provides authoritative support to the certification made by the organization owner.

Clicking on the **Last Evaluation Result** icon, takes you to the details of that evaluation.

Ineffective Processes corresponds to the total of all processes within the organization that were evaluated as having an evaluation other than one tied to the "Effective" opinion.

Unmitigated Risks and **Ineffective Controls** numbers are from the most recent evaluation of the processes and orgs in the certification. **Unmitigated Risks** corresponds to the total of all risks associated with these process and orgs that were evaluated as having a risk tied to an opinion other than the "Mitigated" opinion. **Ineffective Controls** corresponds to the total of all controls associated with these processes and orgs that were evaluated as having a control other than one tied to the "Effective" opinion.

You may click on any of these values to drill down to the details of the process, risk or control.

Note: For more information on the mitigated and effective opinions, refer to Opinions Framework in Oracle Internal Controls Manager, page 8-29.

Open Findings: The "Findings" that are associated with this organization as well as the processes (and associated risks and controls) in the organization. All Findings logged during the audit engagements that encompass this organization will be displayed.

Note: For more information, refer to Findings in Oracle Internal Controls Manager, page 12-1.

Open Issues: The "Issues" that are associated with this process. Issues are similar to Findings and are made in the context of certifying processes. They are logged during process certification by the process owner. Based on their nature and scope, processes with outstanding issues can be certified as "Certified with Issues."

The global operations controller can override any certification by clicking the "certify" icon and entering a certification result.

Note: Also refer to Certification Notes, page 10-19.

My Processes

This window provides a comprehensive "dashboard" view of all processes in the scope of the certification along with their associated evaluations and certifications. As noted earlier, the Global Operations Controller views all processes in all organizations while others view only the processes they own or processes within organizations that list them as the organization owner.

If the process is a corporate process (distinguished by a globe icon), you may drill into it in this window. Oracle Internal Controls Manager then displays a detailed listing of all the local processes (having the same name as the corporate process) in all organizations.

Clicking on the Last Evaluation result icon, takes you to the details of the evaluation. Clicking the History icon immediately next to the Last Evaluation Result, takes you to the Process Evaluation History window where you can view the history and results of all audit engagements where this process was evaluated in the past.

Unmitigated Risks and Ineffective Controls numbers are from the most recent evaluation of the process. Unmitigated Risks corresponds to the total of all risks associated with this process that were evaluated as having a risk tied to an opinion other than the "Mitigated" opinion. Ineffective Controls corresponds to the total of all controls associated with this processes that were evaluated as having a control other than one tied to the "Effective" opinion.

You may click on either of these to drill down to the details of the risk or control.

Note: For more information on the mitigated and effective opinions, refer to Opinions Framework in Oracle Internal Controls Manager, page 8-29.

The Certification and Evaluation Results can be accompanied by icons. The **AMW: Display option for evaluation and certification** profile option specifies whether you want the evaluation and certification columns to be image, text, or both.

Open Findings: The "Findings" that are associated with this process. All Findings logged during the audit engagements that encompass this process will be displayed.

Note: For more information, refer to Findings in Oracle Internal Controls Manager, page 12-1.

Open Issues: The "Issues" that are associated with this process. Issues are similar to Findings and are made in the context of certifying processes. They are logged during process certification by the process owner. Based on their nature and scope, processes with outstanding issues can be certified as "Certified with Issues."

The global operations controller can override any certification by clicking the "certify" icon and entering a certification result.

Assessments: You can create Assessments of processes with respect to process control structure and compliance that can be linked to the process being certified.

Note: Also refer to Certification Notes, page 10-19 at the end of this section.

2. Create a Certification and Set its Scope

A certification is a container and represents a compilation of processes undergoing certification. This certificate may be thought of as a high level node with all of the firm's processes under it.

| Topic | Navigation Path |
|--|---|
| Global Operations Controller view of process certification | Using the Global Operations Controller responsibility, click the Business Process tab. In the Certifications subtab window, click the Create button. |

The following table provides further information on select fields in the Create Certification window.

| Field | Details | Seeded Values | Lookup Type | Accessibility Level |
|-------------------------|---|---------------|-------------|---------------------|
| Auto Reminder (in Days) | <p>To send an automatic notification once every entered number of days to all process owners who have processes that are not yet certified.</p> <p>The notification lists the uncertified processes in both the application welcome window as well as e-mail (if the latter is configured to receive notifications)</p> | NA | NA | NA |
| Certification Owner | <p>The individual responsible for this certification.</p> <p>Certification owners typically have global operations controller access to follow through with organizations pending certification.</p> | NA | NA | NA |

| Field | Details | Seeded Values | Lookup Type | Accessibility Level |
|----------------------|--|--|-------------|---------------------|
| Type | Process certification geared towards 302 or 404 compliance. | SOX 302 SOX 404 | NA | System |
| Certification Period | <p>The LOV lists the accounting periods from Oracle General Ledger.</p> <p>The calendar that these periods are taken from is based on the profile option AMW: Calendar - Q. Periods for certification purposes in Oracle Internal Controls Manager are based on the calendar entered for this profile setting.</p> | According to the Oracle General Ledger calendar. | NA | NA |

All certifications are created in "Draft" status. Before process owners can be notified or processes certified, the status of the certification must be changed to "Active." To do this click the Update button in the Certification Details window (Business Processes tab > Certifications subtab > Drill into the details of the certification).

The following table lists the details of status values in the Update Certification Status window.

| Status | Details |
|-----------|---|
| Draft | All certifications are created in Draft status |
| Active | <p>In order to certify processes and send notifications, certifications must be in Active status.</p> <p>Also, the concurrent programs that summarize and update certification data, only work on processes within "Active" certifications.</p> |
| Completed | Certification is assumed complete. The concurrent program will not work on processes within "Completed" certifications. |
| Rejected | Process certification terminated by the user. |
| Archived | Certificate is ready for archiving. |

Set the Scope of the Certification

After creating the process certification, your next task is to define its scope. The scope determines which entities and processes are included in the certification and therefore defines boundaries to the certification context. Once this is resolved, the Global Operations Controller can initiate launching notifications to process owners to certify their processes.

Note: Setting the scope for a certification is exactly the same as that for an Audit Engagement. For detailed information refer to Set the Scope of the Audit Engagement, page 8-13.

Note that in the "Create Certification" window, the application gives you the option to include all processes and orgs into the scope of the certification.

3. Send Notifications to Business Process Owners

As a global operations controller, there are two ways you can initiate notifications to certify/re-certify processes in Oracle Internal Controls Manager:

1. Run the concurrent program Process Certifications Reminder. This program sends notifications to all process owners in all organizations regarding processes they own that are not yet certified in the current certification period. The notification is sent based on the setting of the Auto Reminder field that is entered when the certification is created.
2. In the My Processes view, you can choose to send individual reminders to process owners. Select individual processes and then click the Send Reminders button to send a notification to those process owners.

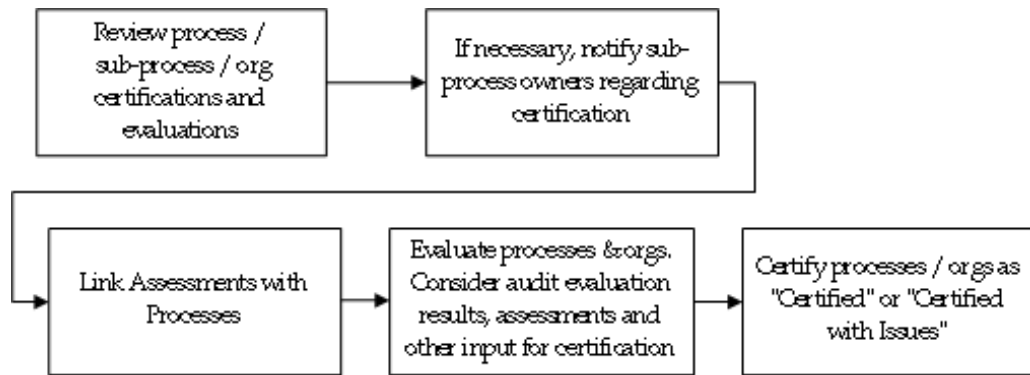
If a process involved in certification does not have an owner, then notifications to certify the process cannot be sent. The global operations controller can certify these processes as appropriate. Note that the result "Certified with Issues" is considered a certification by the application and process owners with processes labelled as such will not receive further notifications.

4. Update Certification Status

In the final step, once certification by process owners is complete, the Global Operations Controller performs a general review and then completes the certification (created in Step 2 above) by updating its status to "Completed." If a certification is listed as "Completed" its processes are excluded from further notifications and computations.

Process / Org Certification: Business Process Owner

The following diagram shows a high level view of the tasks performed by a process owner towards certifying the firm's business processes and organizations. By providing a consolidated view of the relevant process with the ability to drill down into sub-processes, you have the information necessary to make an informed decision regarding certification.



These tasks are listed below.

Review Process and Org Certifications and Evaluations

As noted earlier, business process owners can only view the details of processes that they own (along with associated sub-processes) or processes within organizations that list them as the organization owner. Oracle Internal Controls Manager provides a consolidated dashboard view of these processes and their certification status. Process owners of higher-level processes can drill down to review the details and certification status of associated sub-processes.

Notify Sub-Process Owners

This notification regarding certification is performed as needed. You may only notify the owners of sub-processes under the processes you own.

Link Assessments with Processes (Optional)

| Topic | Navigation Path |
|---|---|
| Use of Assessments in Process Certification | <p>Using the Business Process Owner (or equivalent) responsibility, click the Business Process tab and then the Certifications subtab.</p> <p>Drill into a Certification to access the My Processes subtab (Assessments column)</p> |

Oracle Internal Controls Manager

Home Business Processes Organizational Design Organizations Risk Library

Certifications Assessments Remediation Findings Issues

Business Processes Certifications

Certification: Q1 2004 Certification

Name: Q1 2004 Certification
 Type: SOX 302
 Count: 01
 Auto Reminder (or Date):
 Description: Certification for Q1 2004

Owner: Trazier, Mr. Landon
 Target Completion Date: 28 Feb 2005
 Year: 2004
 Status: Active

My Processes Issues Assessments

View: Assessment

Search

Filter: [Text Box] Audit Location: Active

Organization: [Text Box] Certification Result: [Text Box] (Go)

Select Processes: (Add Reminder) (Remove Assessment)

| Select Name | Organization | Sub Process | Org Process | Certification Result | Last Evaluation | Evaluation History | Unmitigated Risks | Ineffective Controls | Open Findings | Open Issues | Assessment | Certification |
|---|--------------|-------------|-------------|----------------------|-----------------|--------------------|-------------------|----------------------|---------------|-------------|------------|---------------|
| <input type="checkbox"/> Sales Order Processing | SALES | | | | | | 250 | 1 | 1 | | | |
| <input type="checkbox"/> Sales Order Processing | SALES | | | | | | | 1 | | | | |

To aid in the certification, Business Process Owners can tie in and view the results of a process assessment. Assessment results can be used along with data on unmitigated risks, ineffective controls, and open findings/issues to determine whether the process can be certified.

By clicking on the Assessments link, process owners can:

- Link a previously completed Assessment or
- Create and link a new Assessment

Note: For detailed information on the setup and implementation of Assessments, refer to Assessments in Oracle Internal Controls Manager, page 7-1.

Note that the Assessment is executed independently from the certification. However, the results of the Assessment can be used to substantiate and provide credibility to the certification. You can only associate one Assessment per process in a given certification.

Evaluate Processes and Orgs

Evaluate your processes and orgs using audit evaluation results, assessments, findings and other inputs. If necessary you can log issues that must be resolved. The results of the most recent audit evaluation can be seen in the My Processes tab of the Certifications window.

Certify Processes and Orgs

Once your evaluation is complete, click the Certify icon to certify your process (My Processes subtab). The status of the encompassing certification must be "Active." To enter a certification for an organization (My Organizations subtab), you must be logged in using the responsibility "Business Unit Certifier" or "Global Operations Controller."

Note that a process owner may certify/override the certification of any and all sub-processes. In lieu of certifying a process, you can log additional issues by clicking the Open Issues icon.

The following table provides further information on select fields in the Certify Process window / Certify Organizations window.

| Field | Seeded Values | Source | Accessibility Level |
|--------------------------------------|------------------------------------|---|---|
| (Certification Result) Conclusion | Certified Certified with Issues | Opinions Framework component for the Organization - Process object (Certification Result component) | Refer to the section: Opinions Framework in Oracle Internal Controls Manager, page 8-29 |
| (Certification Result) Conclusion | Certified Certified with Issues | Opinions Framework component for the Organization (Certification Result component) | Refer to the section: Opinions Framework in Oracle Internal Controls Manager, page 8-29 |

Note: For more information on seeding certification values, refer to the Opinions Framework in Oracle Internal Controls Manager, page 8-29.

The details of the tasks mentioned above mirrors those described in the section Process / Org Certification: Global Operations Controller with the following exceptions:

- Drilling into a certification will only display those processes that are owned by the process owner or processes within organizations that list them as the org owner.
- While process owners can and must certify their processes, they do not have the ability to update the status of the overall certification (the container that represents a compilation of all processes undergoing certification).
- Business Process Owners cannot view the Dashboard and Scorecard tabs to obtain a summary view of the audit and certification status across all organizations in the enterprise.

Certification Notes

Profile AMW: Display option for evaluation and certification numbers

The numbers in the windows (for ineffective orgs, processes, etc.) are displayed according to the profile option "AMW: Display option for evaluation and certification numbers." Choose from the profile option values seeded as follows:

- Ineffective (Unmitigated)
- Ineffective (Unmitigated) / Total Evaluated
- Ineffective (Unmitigated) / Total
- Ineffective (Unmitigated) / Total Evaluated / Total
- Percent of ineffective over total (Default value)

(Ineffective refers to Organizations, Processes and Controls, Unmitigated refers to Risks)

AMW: Display option for evaluation and certification

This profile option specifies whether you want the evaluation and certification columns to be image, text, or both.

Business Event Processing

Whenever evaluation, certification, and exception data is created or updated in Oracle Internal Controls Manager, that entry raises a business event. Behind the scenes, multiple event subscribers take note of the change and update the source values for the application's engagement and certification views. The numbers hence reflect the latest data and state of the module.

In case of problems with event processing, the concurrent program "Populate Process Certification Summary" can be run to update the numbers. This program summarizes process data and audit evaluation results and then updates the relevant tables in the application.

Note that the application pages display in a disconnected http mode. Hence though the numbers are updated nearly instantaneously in the database tables through event processing, the screen must be refreshed or the page revisited for the changes to display.

Note on Threshold values

The fractional values in columns like Sub-processes and Org Processes are accompanied by an icon. This icon is based on the limits listed below:

| Threshold Value | Image |
|-----------------|-------------------------------|
| 0 - 10 | Checkmark icon (green) |
| 11 - 30 | Warning icon 1 |
| 31 - 80 | Warning icon 2 |
| 81 - 100 | Critical indicator icon (red) |

As an example, assume the fraction in the Sub-Processes column is "99/100" i.e. this is the ratio of the number of sub-processes certified to the total number of sub-processes under this parent. This translates into a 1/100 uncertified value equivalent to 1% and falls under the limits of "0 - 10." The icon next to the fraction is therefore a green checkmark. By providing these color indicators of auditor evaluations, the application provides an easy to read dashboard view of the results of process evaluations and certifications in the enterprise.

Creating and Resolving Issues in Certification

Issues are similar to Findings and are made in the context of certifying processes. They may be defined as nonconformities to established standards in the execution of processes. The nonconformities typically take the form of items of material concern that violate sound procedures and accountability.

Issues are logged during process/org certification by the process/org owner. Their implementation in Oracle Internal Controls Manager is as follows:

- Setup of Issues
- Recording Issues in Oracle Internal Controls Manager

- Using Remediations in closing Issues

Note: The steps listed above are similar to those that are executed for a Finding. For more information, refer to Findings in Oracle Internal Controls Manager, page 12-1.

Financial Statement Certification

This chapter covers the following topics:

- Introduction
- Overview
- Setup of Financial Certifications in Internal Controls Manager
- Certifying Financial Statements using Internal Controls Manager

Introduction

Both internal and external audits can be oriented towards different goals resulting in different types of audits. The financial audit is conducted to determine whether a firm's financial statements are in compliance with specified criteria. Typically these criteria are generally accepted accounting principles although it is also possible to execute financial audits using a cash or other basis.

Whatever the criteria that are used, the central purpose of a financial audit is the certification of financial statements. This chapter provides detailed information on using Oracle Internal Controls Manager in certifying financial statements.

Note: The certification of financial statements makes extensive use of results from the certification of business processes. Once Global Operations Controllers and process owners have certified relevant businesses processes in the enterprise, Signing Officers can perform financial certifications.

For more information, refer to Process Certification, page 10-1 in Oracle Internal Controls Manager.

Overview

To certify a financial statement, the impact on the statement from the different business processes that affect the statement needs to be understood.

Financial statements are comprised of financial items. Each financial item is an account or consolidation of accounts and an integral part of the processes that affect it. It is imperative that the processes behind financial items be recognized and incorporated into the financial audit. Financial audits therefore include both test of details of balances as well as audits of the processes that affect those balances.

In addition, governmental regulation in several countries, for example Section 302 of the Sarbanes-Oxley Act in the USA, requires that the principal officers of a firm certify the

information contained in the firm's quarterly and annual reports. Management must now attest to the effectiveness of internal controls over financial reporting.

The ordinance also requires these officers to certify that:

- They are responsible for establishing, maintaining, and regularly evaluating the effectiveness of the company's internal controls.
- They have made certain disclosures to the issuer's auditors and the audit committee of the board of directors about the issuer's internal controls.
- They have included information in the issuer's quarterly and annual reports about their evaluation and whether there have been significant changes in the issuer's internal controls or in other factors that could significantly affect internal controls subsequent to the evaluation.

To this end, a view of all controls established, internal as well as those specifically implemented for financial disclosure is required for certification of the firm's financial statements. Monitoring of the controls in the various processes impacting the financial statement takes on increased importance and companies need to establish this ongoing monitoring as part of the financial audit.

Successful completion of an audit of these processes and any related follow-up activities which may be required, results in the financial item being "certified." The certification attests to the processes behind the financial item having satisfactory controls in place.

With the financial statement certification functionality in Oracle Internal Controls Manager, signing officers now have a structured way of ensuring that the internal controls related to every account/financial item is working. The adequacy of internal controls within business processes that affect financial statements is brought about from two different inputs:

- For each financial item, the results from internal audit evaluations of the processes affecting that item are presented in a consolidated fashion to financial "signing" officers.
- Also brought into context are the results of the relevant process certifications by the process owners.

These inputs present adequate perspective for the signing officer to evaluate the processes behind the numbers and hence decide whether adequate controls are in place.

Ongoing requirement

As a certification is considered valid for a particular time frame, financial items must be audited on a periodic basis to ensure that they are accurate as of the date of the financial statements. Governmental ordinances typically require certification on a quarterly basis prior to the filing of financial statements with regulatory bodies.

Input from the Audit Engagement

Though some processes are audited infrequently or not at all, the majority of significant business processes in the entity that affect financial items must be subject to a periodic audit. As noted in an earlier chapter, the audit engagement represents a compilation of audit assignments for the entity and is typically associated with the audit of a process. The audit engagement gathers evidence indicating whether the process is fully functional and has satisfactory controls in place.

Setup of Financial Certifications in Internal Controls Manager

There are two steps that must be undertaken to enable financial certifications in Oracle Internal Controls Manager.

- A. Link Financial Items with Business Processes
- B. Import the Financial Statements to be Certified
- C. Setup Significant Account Assertions

A. Link Financial Items with Business Processes

Financial items comprise financial accounts and account summaries. As noted earlier, certification of these items is based in part on the audits of the processes that bear on those financial accounts. It is critical that the processes behind financial items be recognized and incorporated into appropriate internal audit engagements.

As a prerequisite therefore, within the Oracle Internal Controls Manager application, all material financial items must be linked with the business processes that affect them. As an example, the Accounts Receivable financial item is affected by a number of order management processes and sub-processes like sales, credit approval, shipping, etc. All of these processes must therefore be associated with the Accounts Receivable item.

In Oracle Internal Controls Manager, you can link multiple financial items to a process and vice versa.

Note: For detailed information on setting this relationship, refer to the section Linking Key Accounts with Processes, page 2-25.

B. Import the Financial Statements to be Certified

| Topic | Navigation Path |
|--------------------------------------|---|
| Import Financial Statement Structure | Using the Signing Officer (or equivalent) responsibility, click the Setup tab and then select the "Identify Financial Statements for Certification" option. |

You can select available financial statements from Oracle FSG or your external financial reporting application, based on the profiles setup in Step A above.

Oracle Internal Controls Manager handles various alternate scenarios associated with financial statement and key account imports. For example, importing a changed financial statement structure will not obliterate a certification taking place on the older version of the structure. Instead, a new certification involving this financial statement will automatically use the new structure.

The financial statements being imported must utilize the value set specified in the **AMW: Natural Account Value Set** profile option. This option defines which financial accounts will be recognized by Oracle Internal Controls Manager if FSG reports are used. If a third party reporting system is used, then this profile option is ignored.

Note: Ensure that the Key Accounts are imported before the import of the Financial Statements. Otherwise the relationship between Financial Items and Accounts will not be defined.

C. Setup Significant Account Assertions

Assertions refer to implied or expressed representations by management about an organization's processes and/or the components of its financial statements.

Auditing standards classify assertions into broad categories such as:

- Existence or Occurrence
- Completeness
- Valuation or Measurement
- Rights and Obligations
- Presentation and Disclosure

The application allows you to assign assertions to individual controls in the risk library.

Note: For more details, refer to Control Attributes, page 4-11.

In addition, you can also link natural accounts (and their roll ups) to specific assertions. For example, a firm can link all significant payables accounts to the "Completeness" assertion.

By mapping payables accounts to this assertion, Oracle Internal Controls Manager gives you the ability to check whether the "Completeness" assertion is addressed by any controls that bear on these financial items.

This helps ensure that existing accounts payable are included in the accounts payable list.

| Topic | Navigation Path |
|--------------------------------------|---|
| Setup Significant Account Assertions | Using a Super User (or equivalent responsibility), navigate to the Risk Library tab and then the Significant Accounts subtab. Click the Update icon for the appropriate account to associate Assertions with it. |

Oracle Internal Controls Manager

Financial Statements | Audit Operations | Registration of Entities | Organizations | Risk Library

Processes | Risks | Controls | Audit Procedures | Significant Accounts | Inquired

Risk Library > Significant Accounts >

Make Assertions to Account: Gain on Sale

Account Name: 4525 Account Name: Gain on Sale

Assertions

Select All | Select None

Select Name

- ☒ Existence or Occurrence
- ☐ Completeness
- ☐ Valuation or Measurement
- ☐ Rights and Obligations
- ☐ Presentation and Disclosure
- ☐ Valuation or Data
- ☐ Accuracy
- ☐ Restricted Access

Certifying Financial Statements using Internal Controls Manager

Signing Officers identify significant financial accounts and sign off that there are adequate controls for the significant processes that impact these financial

accounts. Execute the following three steps to certify financial statements using Oracle Internal Controls Manager:

1. Create / Review Financial Certifications in the Enterprise
2. Evaluate and Certify Financial Items
3. Certify the Financial Statement

Note: To ensure that numbers in the financial certifications windows described below reflect the latest evaluations, and certifications data, Oracle Internal Controls Manager utilizes business event processing to capture and process changes in the application. Refer to Certification Notes, page 10-19 for more information.

In addition, the concurrent program "Populate Financial Statement Certification summary" can also be scheduled in case of problems with event processing. This program summarize process data and audit evaluation results and then updates the relevant tables in the application.

1. Create / Review Financial Certifications in the Enterprise

Create a Financial Statement Certification

Signing officers who want to get their financial statements certified can create financial statement certifications. A financial statement certification is a container, analogous to a project, and represents a particular financial statement undergoing certification.

| Topic | Navigation Path |
|---|---|
| Creating Financial Statement Certifications | Using the Signing Officer or equivalent responsibility, navigate to the Financial Statements tab and then the Certifications subtab to access the Create button |

Home Financial Statements Business Processes Organizations Setup

Certifications Remediation Findings Issues

Financial Statements: Certifications >

Create Certification

* Indicates required field

* Name

* Owner

Type

Description

* Financial Statement

* Period

* Target Completion Date

Cancel Apply

Include Process Certifications

Process Certifications

Name Go

More Search Options

Included Certifications

Move Move All Remove Remove All

The following table provides further information on select fields in the Create Certification window.

| Field | Details | Seeded Values | Lookup Type | Accessibility Level |
|-------|--|--------------------|-------------|---------------------|
| Type | Financial statement certification geared towards 302 or 404 compliance. | SOX 302 SOX 404 | NA | System |
| Owner | The individual responsible for this certification. The Target Completion Date and Status of the Certification are maintained by the owner. | NA | NA | NA |

| Field | Details | Seeded Values | Lookup Type | Accessibility Level |
|---------------------|--|---------------------------------------|-------------|---------------------|
| Financial Statement | Select the financial statement that this certification encompasses. All financial items that belong to this statement are evaluated. A financial statement certification is a consolidated evaluation of these individual financial items. | Originate in FSG or 3rd party reports | NA | NA |

| Field | Details | Seeded Values | Lookup Type | Accessibility Level |
|------------------------|---|---|-------------|---------------------|
| Certification Period | <p>The LOV lists the accounting periods from Oracle General Ledger.</p> <p>The calendar that these periods are taken from is based on the profile option AMW: Calendar. Periods for certification purposes in Oracle Internal Controls Manager are based on the calendar entered for this profile setting.</p> | According to the Oracle General Ledger calendar. | NA | NA |
| Process Certifications | <p>Select process certifications for which detailed results will be displayed in the certification windows. Note that you can link multiple process certifications for the same financial statement and certification period.</p> <p>The financial items can then be evaluated as "effective" or "ineffective" based on these results i.e. whether the processes impacting them have effective controls in place.</p> | All process certifications that have been saved in the system | NA | NA |

All certifications are created in "Draft" status. Before financial items and statements can be certified, the status of the certification must be changed to "Active." To do this click the Update button in the Certification Details window (Financial Statements tab > Certifications subtab).

The following table lists the details of status values in the Update Certification Status window.

| Status | Details |
|----------|--|
| Draft | All certifications are created in Draft status |
| Active | In order to certify financial items and statements, certifications must be in Active status. Also, the concurrent programs that summarize and update certification data, only work on financial items within "Active" certifications. |
| Rejected | Certification terminated by the user. |

Review a Financial Statement Certification

Review the current status of your financial statement certifications as shown below.

| Topic | Navigation Path |
|---|---|
| View Financial Statement Certifications | Using the Signing Officer or equivalent responsibility, click the Financial Statements tab and then the Certifications subtab |

This window lists all financial certifications that have been initiated in the enterprise. Drill down into a certification to access its financial items. All financial items that belong to the statement linked to this certification can be evaluated and the certification is ultimately a consolidated evaluation of these individual financial items.

Note: By selecting a particular financial statement to be associated with a financial statement certification, the scope of the certification is automatically restricted to the financial items listed under that financial statement.

You can drill into a certification (by clicking on the certification hyperlink) to view

- The financial items that make up the financial statement
- The processes, organizations, risks, and controls affecting these financial items

Oracle Internal Controls Manager collates all the necessary information into a certification dashboard, scorecard, and other views to provide a comprehensive summary of financial items and processes affecting those items.

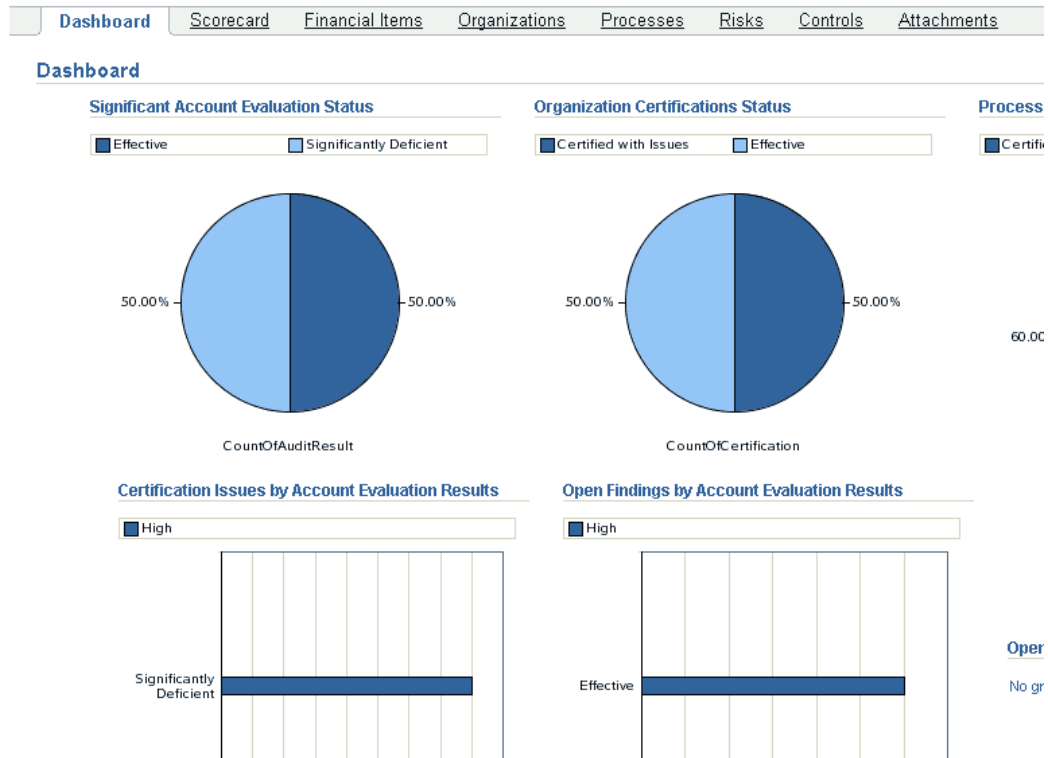
Note: Detailed information on the certification dashboard, scorecard, etc. are provided in the following sections.

2. Evaluate Financial Items

Drill into a particular financial statement certification to evaluate and certify it as follows:

Dashboard Tab

The dashboard provides a summary view of audit evaluation results and certifications for the financial items included in the certification.



The Dashboard has six sections as follows:

- Significant Account Evaluation Status
- Organization Certifications Status
- Process Certifications Status
- Certification Issues by Account Evaluation Results
- Open Findings by Account Evaluation Results
- Open Remediations by Account Evaluation Results

Scorecard Tab

Financial Statement Certification: Balance Sheet Certification - Q4

[Update](#)

| | | | | |
|-------------|---|--|------------------------|--------------------------------|
| Name | Balance Sheet Certification - Q4 | | Owner | Frazier, Mr. Landon |
| Type | SOX 302 | | Target Completion Date | 31-May-2005 |
| Quarter | Q2 | | Year | 2005 |
| Status | Draft | | Financial Statement | Corporate Balance Sheet |
| Description | Balance Sheet Certification - Q4 | | | |

[Dashboard](#)
[Scorecard](#)
[Financial Items](#)
[Organizations](#)
[Processes](#)
[Risks](#)
[Controls](#)
[Attachments](#)

[▼ Certification Result](#)
[Update](#)

[Summary](#)
[Result](#)
[Details](#)

[▼ Ineffective Financial Items](#)

| Financial Item | Last Evaluation |
|---------------------------------|-----------------|
| Cash | ⚠ |
| Cash and Short Term Equivalents | ⚠ |
| Accounts Receivable Total | ⚠ |

[▼ Summary](#)

Last Refreshed On: **06-May-2005 11:26:13**
[Changes To Processes Since \(01-May-2005\)](#)

New Risks Added **0**
 New Controls Added **0**

[Process Certification](#)

| | |
|--|---|
| Corporate Processes Not Certified 3 | Corporate Processes Certified With Issues 2 |
| Organization Processes Not Certified 16 | Organization Processes Certified With Issues 1 |

[Audit Evaluation](#)

| | |
|---|-------------------------------|
| Corporate Processes With Ineffective Controls 3 | Unmitigated Risks 0 |
| Organization Processes With Ineffective Controls 1 | Ineffective Controls 7 |

[▼ Process Certifications](#)

| Name | Type | Certification Owner | Quarter | Year | Status | Creation Date | Target Completion Date |
|-------------------------------|---------------------|---------------------|---------|--------|-------------|---------------|------------------------|
| Q1 2004 Certification SOX 302 | Frazier, Mr. Landon | Q1 | 2004 | Active | 09-Dec-2004 | 31-Dec-2004 | |

This window displays a comprehensive view of the state of the financial statement certification to Signing Officers. For the applicable certification, the Scorecard view provides:

- A financial certification result
- A listing of "ineffective" financial items within the financial statement.
- Changes to processes affecting the financial statement (since the beginning of the certification period). This is a summary view of any additions in risks or mitigating controls associated with these processes since the start of the certification period.

Metrics are also provided from two different perspectives as follows:

- A process certifications summary view of the processes affecting the financial items/statement. This view provides the perspective of the owner of these processes and lists the number of processes that are uncertified or certified with issues in the enterprise.

Note: Also refer to Corporate Processes vs. Organization (Local) Processes, page 10-3.

- The evaluation results from audit engagements involving processes that affect the statement. These results provide an internal audit perspective to the financial statement certification.

Displays the number of processes (Corporate and Organization) with "Ineffective Controls" and "Unmitigated Risks." These numbers are from the most recent evaluations of the respective processes across audit engagements.

The information in the Scorecard tab is similar to the one displayed in a business process certification. Note that the Scorecard tab includes only those processes and organizations that affect the financial items under the financial statement in scope.

Click the Update button to enter or update a certification result.

The following views provide comprehensive summaries of the particular financial items and statement undergoing certification. You can use these views to obtain a comprehensive appraisal of the financial item before entering an evaluation.

Financial Item View - Evaluation Summary

Financial Item views list all financial items belonging to the statement in the certification and provide different perspectives to the evaluator.

The functionality represented in the Evaluation Summary is the following: signing officers can evaluate each financial item in the statement, based on the perspective of:

- The business processes impacting the item and
- The internal control evaluations of those processes

Details from internal audit evaluations present the outstanding problem areas in the respective processes. These include unmitigated risks and ineffective controls. Similarly, the process certification results that are of concern (processes certified with issues or processes that are pending certification) are highlighted.

Process certification in Oracle Internal Controls Manager therefore "flows" into a signing officer's view on line items in financial statements. The signing officer can drilldown into the process (discussed in the sections on Process/Risks/Controls Views) that supports a particular financial line item. The audit evaluation along with a certification provides two independent views of the process.

All numbers can be represented with icons to represent the impact levels. These images can be customized and they filter through all the certification screens in process and financial statement certification.

Note: For more information on the numbers and icons associated with these columns, see Certification Notes.

The profile option "AMW: Show Financial Items with no Control Assertions, Components and Categories" can be set to "No" to omit such financial items from all views.

The financial items can be evaluated as "effective" or "ineffective" based on whether the processes impacting them have effective controls in place. There may also be issues that need to be followed up on.

internal audit staff and provides authoritative support to the certification made by the signing officer.

Unmitigated Risks corresponds to the ratio of the number of unmitigated risks out of the total number of risks that affect the processes associated with the financial item. An unmitigated risk is one that has been evaluated as such by internal audit (a risk having an opinion other than the "Mitigated" opinion).

Ineffective Controls corresponds to the ratio of the number of ineffective controls out of the total number of controls that affect the risks and processes associated with the financial item. An ineffective control is one that has been evaluated as such by internal audit (a control having an opinion other than the "Effective" opinion).

You may click on either of these to drill down to the details of the risk or control.

Note: For more information on the mitigated and effective opinions, refer to the following:

- Step 2: Provide a consolidated evaluation of the control, page 8-22
- Step 3: Evaluate risks based on evaluations of the controls mitigating those risks, page 8-23
- Opinions Framework in Oracle Internal Controls Manager, page 8-29

Evaluate: After checking the remaining views of the financial item (discussed in the following sections), click the Evaluate icon to enter an evaluation of the financial item. The evaluation is tied to the "opinions framework" in Oracle Internal Controls Manager. The following table provides further information on select fields in the Evaluate Financial Item window.

| Field | Seeded Values | Source | Accessibility Level |
|-------------------------------|---|---|---|
| (Audit Opinion) Conclusion | Effective Deficient Significantly Deficient Materially Weak | Opinions Framework components for the Financial Item object (Audit Opinion component) | Refer to the section: Opinions Framework in Oracle Internal Controls Manager, page 8-29 |

Note: For more information on seeding certification values, refer to the Opinions Framework in Oracle Internal Controls Manager, page 8-29.

You may also drill into a financial item to view and certify the financial accounts that make up that item.

Financial Item View - Control Categories

| Dashboard Scorecard Financial Items Organizations Processes Risks Controls Attachments | | | | | | | | |
|--|--|--|-------------------------------------|---|--------------------------------------|------------------------------|-----------------|----------|
| * View By Control Categories | | | | | | | | |
| Expand All Collapse All | | | | | | | | |
| | Financial Items | Effectiveness and efficiency of operations | Reliability of Financial Statements | Compliance with applicable laws and regulations | Safeguarding Information and Systems | Meeting Strategic Objectives | Last Evaluation | Evaluate |
| | Corporate Balance Sheet | | | | | | | |
| | Cash and Short Term Investments | 21% | 6% | 21% | 13% | | | |
| | Accounts Receivable - Net of Allowance | 100% | 0% | 100% | 50% | | | |
| | Other Current Assets | | 0% | | | | | |
| | Net Income for Current Year | | 0% | | | | | |

Controls can be associated with Control Categories (Control Objectives) in the risk library of the application.

Note: For more details, refer to Control Attributes, page 4-11.

As a result of this link, accounts are also linked to Control Categories through the account - process - risk - control matrix. The Control Categories view of a financial item displays the effectiveness (ineffectiveness) of the processes in the enterprise that have controls which address the Control Categories in question.

The dashboard can be read as follows: Of the controls that address this particular Control Category (shown in the column header) and are linked to processes associated with this financial item, X% are ineffective.












Financial Item View - COSO Components

As in the case of Control Categories above, controls can also be associated with COSO components in the risk library of the application.

As a result of this link, accounts are also linked to COSO components through the account - process - risk - control matrix. The COSO components view of a financial item displays the effectiveness (ineffectiveness) of the processes in the enterprise that have controls which bear on the COSO components in question.

The dashboard can be read as follows: Of the controls that bear on this particular COSO Component (shown in the column header) and are linked to processes associated with this financial item, X% are ineffective.

Financial Item View - Control Assertions

| Dashboard | Source | Financial Items | Organizations | Processes | Rules | Controls | Statements | | |
|---|-------------------------|---|---------------|-----------------------|---|-----------------------------|-------------------|-----------------|---|
| View By | | Control Assertions | | | | | | | |
| Expand Collapse | | | | | | | | | |
| Focus Financial Items | Existence or Occurrence | Completeness | Measurement | Risks and Obligations | Presentation and Disclosure | Validation of Data Accuracy | Restricted Access | Lost Evaluation | Evaluate |
|  Corporate Balance Sheet | | | | | | | | | |
|  Cash and Short Term Investments | | 20%  | | | 30%  | | | |  |
|  Accounts Receivable - Sales Allowance | | 50%  | | | | | | |  |
|  Other Assets - Long Term | | 10%  | | | | | | |  |

Controls can be associated with Control Assertions in the risk library of the application. As a result of this link, accounts are also linked to COSO components through the account - process - risk - control matrix.

In addition, accounts are linked to Control Assertions directly through the setup of Account Assertions.

Note: For more details, refer to Setup Significant Account Assertions, page 11-4.

The Control Assertions view of a financial item displays the effectiveness (ineffectiveness) of the processes in the enterprise that have controls which bear on the Control Assertions in question.

The dashboard can be read as follows: Of the controls that address this assertion (shown in the column header) and are linked to processes associated with this financial item, X% are ineffective.

In addition, if the assertion exists for the account (fin item) and is not addressed by any controls on processes that are associated with the financial item, the account or item is still flagged with a 0%. This latter functionality is a result of the setup of the Account - Assertions association and does not apply to the numbers for Control Categories and Control Components. For example, if a Control Category is not addressed by any controls on processes that are associated with the financial item, the display in the grid is simply NULL (blank).

Organizations View

Alternately, a signing officer can perform certification work by surveying the different organizations in scope for the particular statement undergoing certification. This is made possible by the "Organizations" tab in the financial statement certification details page.

This view summarizes the audit evaluations and process certifications from the perspective of all organizations that execute processes that impact the statement. Officers can drill down to the specific processes and their process certification and audit evaluation details to gain an understanding of any processes that have reported problems in their controls. This layout just gives an alternate view of the same information as

under the "Financial Items" tab, but categorized by organization. The officers would then, need to go back to the financial items tab to evaluate the items.

Alternate Views

Alternately, a signing officer can execute certification work by surveying the different processes, risks, and controls in scope for the particular statement undergoing certification. This is made possible through the "Processes," "Risks" and "Controls" tabs described below.

Processes View

The "Processes" tab summarizes the audit evaluations and process certifications from the perspective of all processes that impact the statement. Officers can drill down to the specific processes and their process certification and audit evaluation details to gain an understanding of any processes that have reported problems in their controls. This layout just gives an alternate view of the same information as under the "Financial Items" tab but categorized by process. The officers would then, need to go back to the financial items tab to evaluate the items.

Sub-processes: Valid for parent processes. The ratio of the number of sub-processes certified to the total number of sub-processes under this parent. You can click on the hyperlink to drill down to the evaluation and certification details of the sub-processes.

Org processes: Valid in parent organizations. The ratio of the number of child organizations where the process (or a variant) has been certified to the total number of organizations under the parent.

Certification Result: Tied to the "opinions framework" in Oracle Internal Controls Manager. The application is pre-seeded with the following values:

- Certified
- Certified with Issues

Note: For more information on seeding certification values, refer to the Opinions Framework in Oracle Internal Controls Manager, page 8-29. The relevant object in this case is the Organization Process object that is a "certification" (not the object that is an "evaluation").

Note that "Certified with Issues" counts as a certified entry in computing the fraction in the Sub-Processes column while processes with no certification result count as "Not Certified."

Last Evaluation: Clicking on the Last Evaluation result icon, takes you to the details of the evaluation.

Evaluation History: Clicking the History icon takes you to the Process Evaluation History window where you can view the history and results of all audit engagements where this process was evaluated in the past.

Controls and Risks Views

The "Controls" and "Risks" tabs provide information on all the controls and the risks that impact the statement by being associated with processes that affect the financial items being considered. Again, this is a different view of the same information categorized by organization or process in the other tabs.

Once all reviews are complete, return to the Financial Items - Evaluation Summary window to evaluate the financial item.

Note: For more information, refer to the Evaluate section under Financial Item View - Evaluation Summary, page 11-12.

3. Certify the Financial Statement

As noted earlier, by selecting a particular financial statement to be associated with a financial statement certification, the scope of the certification is automatically restricted to the financial items listed under that financial statement.

Based on the evaluation and certification of individual items within the financial statement, Signing Officers can certify the statement as follows.

| Topic | Navigation Path |
|-----------------------------|--|
| Certify Financial Statement | Using the Signing Officer or equivalent responsibility, click the Financial Statements tab and then the Certifications subtab Drill into the Financial Statement Certification and click the Update button. |

The following table provides further information on select fields in the Certify Financial Statement window.

| Field | Seeded Values | Source | Accessibility Level |
|-----------------------------------|------------------------------------|--|---|
| (Certification Result) Conclusion | Certified Certified with Issues | Opinions Framework component for the Financial Statement object (Certification Result component) | Refer to the section: Opinions Framework in Oracle Internal Controls Manager, page 8-29 |

Findings in Oracle Internal Controls Manager

This chapter covers the following topics:

- Introduction
- Findings in Oracle Internal Controls Manager
- Issues in Oracle Internal Controls Manager
- Correction Requests in Oracle Internal Controls Manager
- Security for Issue Management Entities

Introduction

"Issue Management" in Oracle Internal Controls encompasses the following entities:

- Findings. During the audit process, nonconformities to established standards are often discovered in the organization. These nonconformities are identified as "Findings" and are typically items of material concern that violate sound accounting practice and accountability. Findings must be effectively addressed and remedied.
- Issues. These are similar to Findings except that they are initiated during the certification of a process.
- Remediations. Remediations are the plans and actions to remedy the problem areas and are used to close Findings and Issues.
- Correction Requests. When a segregation of duties violation is discovered, you can initiate a formal Correction Request to correct the violation. The request can be assigned to a particular user and then tracked in the application.
- Disclosure Committees. Provides a structured framework to manage the needs of audit committees.

This chapter provides all the information you need to set up and create the above entities using Oracle Internal Controls Manager.

Note: Detailed information is provided for the set up and implementation of the Findings entity. The set up of the remaining entities mirrors that described for Findings.

Findings in Oracle Internal Controls Manager

Findings encapsulate information on non-compliance that arise in different aspects of the internal audit and assurance system. They are uncovered through audit projects as well

as by random observations. Identified findings are logged by process owners/auditors into the system and can be assigned to other personnel as well. The ability to record and track Findings is critical for capturing information that can materially affect a certification or an audit opinion.

This data is also indispensable for subsequent process work and audit planning activities. Corrections and improvements must be made if nonconformities or opportunities for improvement are discovered. The audit process may therefore be used to drive improvement throughout the organization and follow-up audits are performed to verify implementation and effectiveness of the corrective action.

Oracle Internal Controls Manager provides a rich set of functionality to help you in the recording and resolution of your Findings.

- Findings can be assigned/reassigned to individuals. You can also escalate a Finding for follow up based on predefined routing templates.
- The Findings framework provides a rich set of seeded attributes that can be entered while logging the Finding. In addition, administrators can also define new attributes to capture additional information.
- Threaded discussion capability allows auditors and their supporting staff to collaborate on a Finding.
- "Remediations" (plans and actions to remedy the problem areas) can be created and subsequently linked to Findings. The goal is to address the problem raised in order for auditors and process owners to close the finding(s) and make a recommendation for certification. In lieu of closure, the auditor can also issue the certification as "Certified with Issues."

Note: For more information on Remediations, refer to Using Remediations in closing Findings, page 12-13.

Findings & Remediations Benefits

- Findings assist in raising important questions that must be resolved before processes and financial statements can be certified.
- Findings & Remediations form part of an audit report that is issued at the end of an audit.
- Findings & Remediation form the basis of communication with the audit committee, management, and other stakeholders in the company.
- Findings from an audit project communicate the "problem" areas to all concerned parties.
- Remediation actions solve the "problem" areas.

Findings Types

Findings are recorded during the course of evaluating organizations, processes, risks, controls, audit procedures, and audit projects. They can incorporate any aspect of firm execution in these areas.

Oracle Internal Controls Manager uses Findings Types to distinguish the different kinds of Findings that you can create. The following types are seeded in the module and you can click on the Finding Types hyperlink (see Setup of Findings > Define Basic Information) to view the list.

| Name of Finding Type | Description |
|----------------------|---------------------------|
| ProjAP | Audit Procedure Findings. |
| ProjCtrl | Control Findings. |
| ProjOrg | Organization Findings. |
| ProjProc | Process Findings. |
| ProjRisk | Risk Findings. |
| ProjStep | Audit Procedure step. |
| Project | Project Findings. |

When a Finding is created, the application automatically logs it as one of these types based on the context in which it was created.

Note: Finding Types are pre-seeded in Oracle Internal Controls Manager. The application does not recognize any other types of Findings.

The following are examples of Findings in an enterprise:

Organization Findings: The organization structure is not conducive to obtaining information and interviews for audits in an easy manner.

Process Findings: In the procure-to-pay process, there is an unidentified risk in terms of a non-employee being vested with decision power to purchase.

Risk Findings: The risk "theft" is impacting multiple processes because of a lack of physical security.

Control Findings: The Control of a manager authorizing purchases could be flouted in some purchases or there may not be proper auditing checks on the efficacy of this control.

The Finding Type drives several parameters associated with the Finding. Drill into a Finding Type to set the following information:

- Default Assigned To information
- Approval Routing
- Attribute Groups

The implementation of Findings in Oracle Internal Controls Manager is discussed in the following sections:

- Setup of Findings
- Recording Findings
- Querying and Viewing Findings
- Using Remediations in closing Findings

Setup of Findings

Before Findings can be created and used in Oracle Internal Controls Manager, they must be set up as described in this section. Note that these setups are undertaken for

a particular Finding Type and all Findings associated with that Type will accordingly display the setups. Define the following for each Finding Type:

1. Basic Information
2. Attributes and Value Sets
3. Finding Priorities and Reasons
4. Approval Routing Templates
5. Configuration

The listed steps are optional and you can create a Finding that does not utilize any of these features.

1. Define Basic Information

All Findings associated with the Finding Type will use this information as a default. Basic information includes valid dates/numbering for the Finding and default "Assigned To" information.

| Topic | Navigation Path |
|---|--|
| Define Basic Information for a Finding Type | Using the Internal Auditor (or equivalent) responsibility, click the Setup tab and then the Issue Management subtab. Select the Categories and Types hyperlink. For the Findings Category click on Types, drill into the appropriate Finding Type and then click on the Basic Information hyperlink. Update this info as required. |

For Autonumbering that is Sequence Generated you may designate an appropriate Prefix.

2. Define Attributes and Value Sets

Oracle Internal Controls Manager allows you to create different attributes (dimensions) that can be attached to different Finding Types. Attribute values can be seeded in Value Sets. This is a powerful feature and allows you to add user defined elements to a Finding based on its Type.

Consider the following examples, all of which relate to creating Findings in a particular context:

- When the Finding is created in a risk context, you may want to add the attribute "Exposure" with pre-defined levels.
- When the Finding is created in the context of an audit procedure, you may want to also set an attribute "Ease of Execution" with pre-defined levels. You may also want to provide the originator with a text box to allow free text regarding this dimension.
- When you create a Finding in the context of a project, you may want to add an attribute "Federal" with values "Yes" or "No."

The following four tasks must be undertaken to define attributes and attach them to a Finding Type:

- a. Define Value Sets and Values

- b. Define Attribute Groups and Attributes. Associate Value Sets to Attributes.
- c. Associate Attribute Groups to Finding Types
- d. Define Pages to display the Attribute Groups

a. Define Value Sets and Values

| Topic | Navigation Path |
|-------------------|--|
| Define Value Sets | <p>Using the Internal Auditor (or equivalent) responsibility, click the Setup tab and then the Value Sets subtab.</p> <p>In the Maintain Value Sets window, click the Create button. You will also define appropriate values from this window.</p> |

b. Define Attribute Groups and Attributes. Associate Value Sets to Attributes.

| Topic | Navigation Path |
|--|--|
| Define Attribute Groups Define Attributes | <p>Using the Internal Auditor (or equivalent) responsibility, click the Setup tab and then the Issue Management subtab</p> <p>Select the Attributes hyperlink</p> <p>In the Search: Attribute Groups window, click the Create button.</p> <p>Once the Attribute Group is created, click the button to Add Attributes. Each of the attributes created can be linked to a value set defined in step a.</p> |

The following table provides further information on select fields in the Create Attribute Groups page.

| Name | Description |
|-----------|---|
| Multi-Row | <p>An attribute group can be multi-row or single-row. Multi-row attribute groups enable you to associate multiple sets of attribute values with the same object instance.</p> <p>For example, if "Exposure" was a multi-row attribute, then you can associate multiple "Exposure levels" with the attribute in the Finding. For Single Row attribute groups, you can enter only one value for each attribute.</p> |

c. Associate Attribute Groups to Finding Types

| Topic | Navigation Path |
|---|--|
| Associate Attribute Groups to Finding Types | <p>Using the Internal Auditor (or equivalent) responsibility, click the Setup tab and then the Issue Management subtab.</p> <p>Select the Categories and Types hyperlink.</p> <p>For the Findings Category click on Types, then drill into the appropriate Finding Type and then click on the Attribute Groups hyperlink. Finally click the Add Attribute Groups button to make the association.</p> |

d. Define Pages to display the Attribute Groups

| Topic | Navigation Path |
|----------------------|--|
| Finding Type details | <p>Drill into the appropriate Finding Type as described in c. above and then click on the Pages hyperlink.</p> <p>Finally, click on the Create Page hyperlink and then the "Add Another Row" button to associate one or more Attribute Groups to the page.</p> |

Note: Creating Attributes and attaching them to Findings uses functionality originally devised in the Oracle Product Lifecycle Management module.

If you need further information on creating Value Sets, Attribute Groups, and Attributes, refer to the following sections in the *Oracle Advanced Product Catalog Implementation Guide*:

Chapter 4: Change Management Administration

Chapter 7: Attributes and Function Administration

3. Define Findings Priorities and Reasons

Findings can have an associated predefined Priority and Reason and you can create/update seeded values for your Findings. When you later create a Finding, you can choose to associate it with one of these predefined values.

| Topic | Navigation Path |
|-------------------|--|
| Findings Priority | <p>Using the Internal Auditor (or equivalent) responsibility, click the Setup tab and then the Issue Management subtab.</p> <p>Click on the Priorities/Reasons hyperlinks to create Priority/Reason values that you can associate with your Findings.</p> <p>In the Issues Management subtab select the Categories and Types hyperlink.</p> <p>For the Findings Category click on Types, then drill into the appropriate Finding Type and select Codes to create a subset of these Priorities/Reasons for use with that Finding Type. When Findings are entered in the system, they can be associated with a Priority/Reason in this subset.</p> |

4. Define Approval Routing Templates

You may escalate a Finding for follow up and/or approval based on predefined routings. For example, a Finding that is recorded in the context of an audit procedure could be assigned to a particular person for further investigation, while one recorded for an audit risk could use a completely different approval hierarchy.

Oracle Internal Controls Manager allows you to create approval routing templates and associate one or more templates to a Finding Type. The template specifies how the Finding needs to be routed and the workflow process is then entirely automated.

Perform the following two steps to implement approval routings.

a. Create an approval template

| Topic | Navigation Path |
|-------------------------------------|--|
| Setup of Approval Routing Templates | <p>Using the Internal Auditor (or equivalent) responsibility, navigate to the Setup tab and then the Approvals subtab.</p> <p>Click the Approval Templates hyperlink and then the Create button.</p> |

In this window, select the Type of the template as follows:

Approval: The Approval workflow template type is valid only for workflows within a Lifecycle that has a status type of Approval.

Definition: The Definition workflow template type is used primarily for workflows within a Lifecycle that has a status type of Open.

Definition and Approval: The Definition and Approval workflow template type is used primarily within a Lifecycle that has a status type of Approval.

Generic: The Generic workflow template type is used for all other Lifecycle status types.

Note: These templates are used in Lifecycle Statuses as described in b. below. For more information on Lifecycle Statuses, refer to Track Lifecycle Statuses, page 12-13.

Then add one or more workflow approval steps based on your requirements. Each of these steps requires the following parameters:

- Workflow Process - "Request Approval," "Request Comment," "FYI."
- Assignee - Assigned from the setup of the template ("Derived") or "User Entered."
- Response Required - Either "All" approve or any "One" approves. Also, if you choose the "Mandatory Assignees" option, then for every assignee, the form requires you to specify whether the assignee is mandatory or optional. No response is required from an Assignee for a "FYI" process.
- Days to Respond - Enter the number of days (from the time this step is executed) in which you need a response.
- Finally, select the Assignee i.e. the recipient of the Finding. The application allows you to choose between "Group," "Person," or "Role." You do not need to select an Assignee if the recipient is "User Entered."

[Risk Library](#) | [Audits](#) | [Issue Management](#) | [Opinions](#) | [Import](#)

[Setup: Issue Management](#) > [Workflow Templates](#) > [Create Workflow Template](#) >

Add Step

* Indicates required field

* Step

Workflow Process

Assignee

Response Required

Days to Respond

Instructions

Assignees

Add Assignee

| Type | Name | Company | Delete |
|-----------------|------|---------|--------|
| No data exists. | | | |

b. Associate the approval template to a Lifecycle Status within a Finding Type.

A lifecycle within Issue Management can be thought of as a sequence of statuses for the applicable Entity.

Note: For more information on Lifecycle Statuses, refer to Track Lifecycle Statuses, page 12-13.

Before the template can be used, it must be associated with a Lifecycle Status within a Finding Type.

| Topic | Navigation Path |
|---|--|
| Associate the approval template to a Finding Type (and set up / complete the Lifecycle) | <p>Using the Internal Auditor (or equivalent) responsibility, click the Setup tab and then the Issue Management subtab.</p> <p>Select the Categories and Types hyperlink.</p> <p>For the Findings Category click on Types, drill into the appropriate Finding Type and then click on the Workflow hyperlink.</p> |

Add an "Approval" status (or any other required status) between the seeded "Open" and "Completed" statuses.

Then update the properties of each status as follows:

- Select a valid status for "promotion" and "demotion" of the workflow step. Once the Finding passes all required Assignees and approvals in a particular status, it can be advanced to the next.
- Associate a status with a template setup in (a) above. Within a status, the Finding is routed according to this template. It is important to remember that a workflow template of type "Approval" can only be linked to a Lifecycle status that itself has a status type of "Approval."

5. Define the Displayed Configuration

The Configuration in Issues Management setup refers to the "Sections" and "Primary Attributes" that are displayed for a Finding summary.

| Topic | Navigation Path |
|---|---|
| Define the Displayed Configuration for a Finding Type | <p>Using the Internal Auditor (or equivalent) responsibility, click the Setup tab and then the Issue Management subtab.</p> <p>Select the Categories and Types hyperlink.</p> <p>For the Findings Category click on Types, drill into the appropriate Finding Type and then click on the Configuration hyperlink.</p> |

The Sections include the following: Dependencies, Action Log, Attached Documents.

Note: For more information on the use of these Sections in a Finding, refer to Recording Findings in Oracle Internal Controls Manager, page 12-9.

Primary Attributes include the following: Description, Assigned To, Priority, Reason, Status etc. Primary Attributes are listed on the Findings Summary screen.

Recording Findings in Oracle Internal Controls Manager

You can enter a Finding in multiple places in the application. In the appropriate window, click the "Open Findings" icon and then the Create button.

The default Finding Type is always based on the context in which the Finding is recorded. For example, if the Finding is entered from the Controls detail page of the audit project, the Finding Type is automatically set as "ProjCtrl."

The following table shows the navigation paths to the various contexts from where you can create the different types of Findings:

| Finding Type | Created From Window |
|--------------------------|--|
| Audit Procedure Findings | Created from the Audit Tasks details window in an audit project. You need to drill into a project task to access the Findings icon associated with an audit procedure. |
| Control Findings | Created from the Control details window in an audit project. |
| Organization Findings | Created from the Organizations and Processes details window in an audit project. |
| Process Findings | Created from the Organizations and Processes details window in an audit project. |
| Risk Findings | Created from the Risk details window in an audit project. |
| Audit Procedure step | Created from the Audit Tasks details window in an audit project. Drill into a project task and then click on the Status to access the Findings icon associated with individual steps of the audit procedure. |
| Project Findings | Created from the Findings details window within an audit project. |

When you create a Finding, several fields display default values based on the setups described in the previous section. For example:

- The "Finding Number" is based on the setup of Basic Information for the Finding Type.
- The routing information in the Workflow Approval subtab also defaults from the setup of the Finding Type. Note that the view in this subtab is for a particular Lifecycle Status. View the Finding Summary page (described in the next section) for a concise view of all status.

Other parameters can be entered using values seeded during setups. For example:

- "Priorities"/"Reasons" are entered using values that you seeded during setup.
- Pages to display Attribute Groups appear as subtabs. Attributes in these windows are entered using values seeded for the associated value sets.

Audits: Projects > Audit Project: Americas OTC Mgmt Q4-2003 >

Create Finding

* Indicates required field

Cancel Save for Later Submit

Finding Type **Project**

Finding Number **PROJECT15**

* Finding Name

Description

Project **Americas OTC Mgmt Q4-2003**

Additional Information Dependencies Workflow Approval Attached Documents Impact and Timeline

* Assigned To Landon Frazier

Priority High

Reason Cost

Requestor Landon Frazier

Need By Date

(example: 16-Sep-2004 19:45:00)

Note: For more information on the subtab sections in the Create Finding window, refer to the following section, Working with Findings in Oracle Internal Controls Manager, page 12-11

Working with Findings in Oracle Internal Controls Manager

There are two levels of querying Findings in the application. When you access the application using the menu path Audit Operations > Engagements > Audit Engagement and initiate/view a Finding in the various details windows, it is a Finding of a particular type within a specific project.

On the other hand, when you enter the application using the menu path Audit Operations > Findings (also exists under Business Processes and Financial Statements tabs), you can query any kind of Finding across projects. As an example, you can choose to view the Findings for a particular control in the prior three months across all projects in the firm.

Once you create a Finding, you can drill into it to access the Finding Summary page. Use this summary page to record information on the Finding as well as initiate actions such as Approval Routings.

Finding Summary: 1234522222

Actions

Finding Type **ProjRisk**
 Finding Number **1234522222**
 Finding Name **adfsf**
 Description **adfsfsf**

Assigned To **Landon Frazier**
 Priority **High**
 Phase **Open**
 Approval Status **Not submitted for approval**
 Project **Americas OTC Mgmt Q4-2003**
 Organization **Sales 1003**
 Risk **Fraudulent Returns**

Requestor **Landon Frazier**
 Need By Date
 Creation Date **15-Sep-2004 16:32:39**
 Reason **Cost**

▶ Action Log

▶ Attachments

▶ Dependencies

▶ Impact and Fines

▼ Lifecycle Phases

| Select | Lifecycle Phase | Current Lifecycle Phase | Workflow/Approval Template | Workflow/Approval Status | Start Date and Time | Finish Date and Time |
|----------------------------------|-----------------|-------------------------|----------------------------|--------------------------|----------------------|----------------------|
| <input checked="" type="radio"/> | Open | ✓ | | | 15-Sep-2004 16:33:23 | |
| <input type="radio"/> | Approval | | Finding Approval Routing | Not Started | | |
| <input type="radio"/> | Completed | | | | | |

Lifecycle Phase: Open

Template Name

Submitted By

Document the Action Log

The Action Log section acts as a bulletin board where you can initiate a discussion thread among the audit team and management. You can:

- Post Comments
- Request Comments from specific users and track these comments from this section. Oracle Internal Controls Manager maintains an exhaustive history of changes and comments in this window.

Display and Update Dependencies (If Any)

The Dependencies container shows all entities that are linked to the Finding. Refer to the section Using Remediations in closing Findings, page 12-13.

Record Attribute Values

The displayed name of this component of the Findings Summary page is based on the nomenclature of the Pages used to contain the Attribute Groups.

Note: For more information on creating Pages, refer to 2. Define Attributes and Value Sets, page 12-4.

As described earlier, Attributes associated with Findings are based on your set up of the associated Finding Type.

Track Lifecycle Statuses

A lifecycle within Issue Management can be thought of as a sequence of statuses (phases) for the applicable Entity. Each status represents a phase that must be evaluated before it can be promoted to the next status. For example, the lifecycle status for the "Project" Finding Type might be: Open, Approval, Completed. Lifecycles enable you to track and control the statuses of the various entities in Issue Management.

You can specify a set of lifecycle statuses for each Type within an Entity Category. Hence the Finding Type "Project" Finding Type can have a different set of lifecycle statuses than the "ProjStep" Finding Type. Similarly each "Issue" Type can have its own implementation of lifecycle statuses.

The setup of a Lifecycle is conducted during the definition of an Approval Routing Template.

Note: For more information, refer to 4. Define Approval Routing Templates, page 12-7.

Initiate the approval routing in the Workflow section of the Findings Summary window. As an example, consider a new finding having an initial Lifecycle status of "Open." When you promote the Finding to the next status (for example, a status of "Approval") the workflow process is launched. If all workflow approvals go through successfully, the Lifecycle status changes to the promoted status.

Using Remediations in closing Findings

Use the Remediations feature to help you in closing your Findings. Remediations encapsulate information on plans and actions that are being undertaken to address the Findings that have arisen in the course of the audit project.

Remediations can be set up with Attributes, Approval Routings, etc. and the set up mirrors that described earlier for Findings.

Note: For more information, refer to the appropriate set up for Findings. Use the "Category and Type" as "Remediation" in the appropriate menu path.

Create the Remediation

Remediations are created from the Findings Summary page of a particular Finding and are therefore automatically linked with that Finding.

| Topic | Navigation Path |
|-----------------------|--|
| Creating Remediations | Using the Internal Auditor (or equivalent) responsibility, click the Audit Operations tab and then the Findings subtab. For the relevant Finding, drill down to the Findings Summary page and then click the create Remediation button. |

To view all Remediations associated with a Finding

Oracle Internal Controls Manager allows you to personalize the display format of your Findings under the Findings subtab.

| Topic | Navigation Path |
|--|--|
| Viewing Dependencies (like Remediations) associated with a Finding | Using the Internal Auditor (or equivalent) responsibility, click the Audit Operations tab and then the Findings tab. Personalize the display format by clicking the Personalize button associated with the Display Format. Disclose the Dependencies container. |

[Audits: Projects](#) >

Audit Project: Americas OTC Mgmt Q4-2003

| | | | |
|----------------|---------------------------|-----------------|------------------|
| Project | Americas OTC Mgmt Q4-2003 | Start Date | 29-Apr-2004 |
| Project Number | 302003 | Project Manager | Abbott, Mr. John |
| Status | Active | | |

[Scope](#)
[Audit Tasks](#)
[Controls](#)
[Risks](#)
[Organizations and Processes](#)
[Findings](#)

[View Reports](#)

Search Criteria: [Go](#) [Personalize](#)
 Display Format: [Go](#) [Personalize](#)
[Create](#)

Select Finding: [Go](#)
Previous 1-10 Next 10

[Show All Details](#) | [Hide All Details](#)

| Select | Details | Name | Number | Need By Date | Action Log | Dependencies | Lifecycle Phases | Impact and Timeline |
|-----------------------|----------------------|--|---------------------|--------------|------------|--------------|------------------|---------------------|
| <input type="radio"/> | Show | Management did not monitor or approve changes in prices | 500 | 25-OCT-04 | | | | |
| <input type="radio"/> | Show | Current prices not reflected in all locations | 501 | 31-MAY-04 | | | | |
| <input type="radio"/> | Show | Original units are not being tracked by Serial Number per company policy | 400 | 25-MAY-04 | | | | |

Drill down into this container to view all Remediations (as well as other entities like Correction Requests, Incident Reports etc.) associated with the Finding. In the Dependencies window you can also select an additional entity (for example another Remediation) through the Add Dependency LOV and link it to the Finding.

Remediations can also be linked to Correction Requests, Incident Reports, Issues, and Disclosure Committee entities in this manner.

Issues in Oracle Internal Controls Manager

Issues are similar to Findings and are made in the context of certifying processes. They may be defined as nonconformities to established standards in the execution of processes. The nonconformities typically take the form of items of material concern that violate sound procedures and accountability.

Issues are logged during process certification by the process owner. Their implementation (setup, recording, viewing, and closing) in Oracle Internal Controls Manager mirrors that described for Findings in the previous section.

Note: For more information, refer to the appropriate set up for Findings. Use the "Category and Type" as "Issue" in the appropriate menu path.

Comparable to Finding Types, Oracle Internal Controls Manager uses Issue Types to distinguish the different kinds of Issues that you can create. When an Issue is created

during certification, the application automatically logs it as one of these types based on the context in which it was created.

| Name of Issue Type | Description | Navigation Path |
|--------------------|------------------------------|--|
| CertIssue | Process Certification Issues | Using the Business Process Owner (or equivalent) responsibility, click the Business Process tab and then the Certifications subtab. Drill down into a certification, then select the Issues subtab. |
| ProcIssue | Process Issues | Using the Business Process Owner (or equivalent) responsibility, click the Business Process tab and then the Certifications subtab. Drill down into a certification, then select the My Processes subtab. |

Note: Issue Type OrgIssue is not used in the application.

Note that you cannot create Remediations (to link to Issues) while working with certifications. Remediations can only be created in a Findings context. However, you can link the Remediation to an Issue as follows:

| Topic | Navigation Path |
|--|---|
| Viewing and linking Remediations with Issues | Using the Business Processes Owner (or equivalent) responsibility, click the Business Process tab and then the Issues tab. Personalize the display format by clicking the Personalize button associated with the Display Format and show the Dependencies container. |

Drill down into this container to view all Remediations (as well as other entities like Correction Requests, Incident Reports etc.) currently associated with the Issue. In the Dependencies window you can also select an additional entity (for example another Remediation) through the Add Dependency LOV and link it to the Issue.

Similarly, you can view all Issues associated with a Remediation by using the menu path Business Process tab > Remediation subtab.

Correction Requests in Oracle Internal Controls Manager

When a segregation of duties violation is discovered, you can initiate steps to correct the violation and therefore mitigate the risk from users having access to incompatible tasks in the organization.

The initiation takes the form of a formal correction request that can be assigned to a particular user and then tracked in the application. You can also record issues that require follow up action.

The setup of Correction requests mirrors that described for Findings. Note that "DutyViolat" is the only Type of Correction Request in the application.

Note: For more information, refer to the appropriate set up for Findings. Use the "Category and Type" as "Correction Request" in the appropriate menu path (you may need to advance to the second set of categories to view "Correction Requests").

Also refer to 3. Initiate Correction Requests, page 9-13 (and subsequently modify user duties)

Security for Issue Management Entities

To ensure the integrity of the internal audit, it is critical that only appropriate and approved users can record, view, and update issue management entities (Findings, Issues, Correction Requests, and Remediations) and their associated data. For example, only approved users should be able to create a Finding or enter responses to it. Responses to the Finding can take the form of requesting or posting comments regarding the Finding, making status updates, initiating approval routings, etc.

The following sections describe the setup and implementation of the security model that is employed for issue management within Oracle Internal Controls Manager. The appropriate implementation of this security model helps to ensure the reliability of the initiation and follow up of items discovered during the course of the audit that require resolution.

Creating New Issue Management Entities

Oracle Internal Controls Manager allows or disallows the creation of new issue management entities based on assigned responsibilities:

- A Super User can create any issue management entity.
- An Internal Auditor can create findings and correction requests.
- Remediations can be created by anyone who can access a Finding using the owner or reviewer access level values (described in more detail below).
- A Global Operations Controller can create issues.
- A Process Owner or Organization Manager (as defined above) can create issues.

Other than by using the above five responsibilities, users cannot create issue management entities in the application.

Profile based access to Issue Management Entities

For controlling access to issue management entities that already exist in the system, Oracle Internal Controls Manager furnishes the following responsibility level profile options:

- AMW: Remediation Access
- AMW: Issue Access
- AMW: Finding Access
- AMW: Correction Request Access

Each of these profiles can be set to one of three values that control access to the various issue management entities as follows:

1. "None" - lowest access level, allows no access
2. "Reviewer" - for read only access
3. "Owner" - for read and update access

The following table displays the profile options and responsibilities with their pre-seeded values:

| Profile Option | Internal Auditor Resp. | Business Process Owner Resp. | Global Operations Controller Resp. | Signing Officer Resp. | Super User Resp. |
|--|------------------------|------------------------------|------------------------------------|-----------------------|------------------|
| Findings (AMW_FINDING_ACCESS) | Owner | None | Reviewer | Reviewer | Owner |
| Issues (AMW_ISSUE_ACCESS) | Reviewer | None | Owner | Reviewer | Owner |
| Remediations (AMW_REMEDIATION_ACCESS) | Owner | None | Owner | Reviewer | Owner |
| Correction Requests (AMW_CORRECTIONREQ_ACCESS) | Owner | None | None | None | Owner |

Note: The seeded values in this table can be configured to meet your requirements. In addition, custom responsibilities that you create can have appropriate values for each of the profiles listed.

Users of the application can obtain more than one level of access to an issue management entity. If a user gets more than one level of access for a particular issue management entity (due to different access rules), the highest level of access prevails. This is explained in more detail below.

Assignee based access to Issue Management Entities

Multiple access levels can occur because an issue management entity that is created during the course of an audit is always assigned to a user. Access levels for assignees are seeded by Oracle and these cannot be changed:

- Findings assignment: Reviewer access (note that the assignee for a Finding can also create remediations for that Finding)
- Issues assignment: Owner access

- Remediations assignment: Owner access
- Correction Requests assignment: Owner access

Example: Assume that a user U logs into the application with a Business Process Owner responsibility and U is the assignee for a Finding F.

Based on the seeded responsibility level profile for a Business Process Owner, the access level of the user for a Finding is "None." However, since user U is an assignee for the Finding F, his access level is also "Reviewer." As the higher of these two levels is "Reviewer," U gets "Reviewer" access for F.

Note that if U was logged in using responsibility Internal Auditor, he would get "Owner" access because "Owner" access at the responsibility level is a higher access level than "Reviewer" access at the assignee level.

Role based access to Issue Management Entities

Multiple access levels can also occur because of the various and distinct roles that a user can possess while creating or responding to issue management entities. These roles take the following forms:

Creator: the user who created the issue management entity.

Process Owner: the user who owns the process (or a parent of the process) against which the issue management entity is logged.

Organization Manager: the user who is the manager of an organization (or the manager of a parent organization) against which the issue management entity is logged.

The following table displays issue management entities and roles with their pre-seeded values and these values cannot be changed:

| Issue Mgt Entity | Creator role | Process Owner role | Org Manager role |
|---------------------|--------------|--------------------|------------------|
| Findings | Owner | Reviewer | Reviewer |
| Issues | Owner | Owner | Owner |
| Remediations | Owner | Owner | Owner |
| Correction Requests | Owner | None | None |

Example: Assume that a user U logs in with Business Process Owner responsibility and U is the process owner against which a Finding F is logged.

Based on the seeded responsibility level profile for a Business Process Owner, the access level of the user for a Finding is "None." However, since user U is the Process Owner of the process against which the Finding F was logged, his access level is also "Reviewer." As the higher of these two levels is "Reviewer," U gets "Reviewer" access for F.

Note that if U was logged in using responsibility Internal Auditor, he would get "Owner" access. This is because "Owner" access at the responsibility level is a higher access level than "Reviewer" access at the Process Owner level.

Note: The site level profile "ENG: Internal User Default Role for Changes" sets the minimum access level for issue management entities in the application. In order for the security described in the above sections to be effective, this profile option value should be set to "None."

The default value is "Reviewer." If this value is not changed to "None" then all users get at least the "Reviewer" access to all entities and the lowest access level effectively becomes "Reviewer."

Control Reports

This chapter covers the following topics:

- Introduction
- Risks with no Controls report
- Controls without Audit Procedures report
- Controls with no Risks report
- Risk Control Matrix report
- Business Process Summary report
- Process Organization Summary report
- Audit Procedures Summary report

Introduction

Oracle Internal Controls Manager provides seven predefined risk library reports that enable you to periodically verify the accuracy and integrity of the processes and objects that are present in your risk library. The reports are listed below:

1. Risks with no Controls report
2. Controls without Audit Procedures report
3. Controls with no Risks report
4. Risk Control Matrix report
5. Business Process Summary report
6. Process Organization Summary report
7. Audit Procedures Summary report

All of the reports are written using Oracle Discoverer and available as Discoverer workbooks. The initial seeded workbooks contain default parameters and Discoverer prompts the user during the execution of the report query for the parameters that are needed.

You may change the results and parameters for the workbooks depending on your custom requirements.

Risks with no Controls report

This report provides details on risks that have no mitigating controls. As an example, you may have a risk that revenue will be released from deferred to regular revenue when contingencies still exist on the revenue. The contingency in this case might be that the customer has the right to return a product for which they have been invoiced if the product fails installation and configuration testing.

Discoverer Workbook Name: AMW Control Reports

Folder Name: Risks with no Controls

Seeded Query: The seeded query will retrieve all risks for which no controls have been associated.

Report parameters and search results

The report has the following default parameters:

- Associated Process Name
- Risk Name
- Risk Description

The default columns of the report are shown below:

- Risk Type
- Risk Name
- Risk Description
- Likelihood
- Impact

The query results are shown in a tabular format with data displayed for the above columns.

Controls without Audit Procedures report

It is important to know the controls that have no audit steps assigned to test them. The previous example listed a potentially risky situation where a revenue would be reclassified from deferred revenue to regular revenue when contingencies affecting it still existed.

This risk can be mitigated by a control. An example of such a control would be that journal entries that have credits to a deferred revenue account must be routed through the legal department for review before approval for reclassifying it is granted. The control however will be ineffective if all requests for such review are delegated to administrative staff without professional oversight. It is therefore critical that all controls be periodically tested with appropriate audit procedures.

Discoverer Workbook Name: AMW Control Reports

Folder Name: Controls without Audit Procedures

Seeded Query: This query will retrieve all the Controls for which no associated Audit Procedures exist.

Report parameters and search results

The report has the following default parameters:

- Risk Name
- Risk Description
- Control Name
- Control Description

The default columns of the report are shown below:

- Risk Type
- Risk Name
- Risk Description
- Impact
- Likelihood
- Control Type
- Control Name
- Control Description

The query results are shown in a tabular format with data displayed for the above columns.

Controls with no Risks report

This report lists controls with no risks. For example, you may have a control that the signature of a manager must be on a printed requisition. This control may have been superseded with Workflow approval of the web based requisition. The control is therefore no longer associated with any risk or process.

Discoverer Workbook Name: AMW Control Reports

Folder Name: Controls with no Risks

Seeded Query: This query will retrieve all the Controls for which there are no associated Risks

Report parameters and search results

The report has the following default parameters:

- Control Name
- Control Description

The default columns of the report are shown below:

- Control Type
- Control Name
- Control Description

The query results are shown in a tabular format with data displayed for the above columns.

Risk Control Matrix report

It is extremely useful to view a single report in matrix form with all the following details:

- The business process
- The risks that the business process is exposed to
- The controls that are used to mitigate the risk
- The procedure for testing the effectiveness of the control

As an example, consider the typical sales process in an organization. One of the risks that the sales process is exposed to is that recorded sales are for shipments actually made to nonfictitious customers i.e. sales transactions in the process are invalid. There could be several controls associated with this risk. For example:

- Recording of sales is supported by authorized shipping documents and approved customer orders
- Monthly statements are sent to customers and complaints receive an independent follow up

Procedures to test the effectiveness of the above controls will include the following:

- Examine records of sales invoices for supporting bills of lading and customer orders
- Examining customer correspondence files

This report provides an auditor, internal or external, the ability to view all of the above details in a single page.

Discoverer Workbook Name: AMW Control Reports

Folder Name: Risk Control Matrix

Seeded Query: This seeded query will retrieve the process, the risks the process is exposed to, mitigating controls for the risks, and the audit procedures associated with the controls.

Report parameters and search results

The report has the following default parameters:

- Process Name
- Risk Name
- Risk Description
- Control Name
- Control Description

The default columns of the report are shown below:

- Process Name
- Risk Type
- Risk Name
- Risk Description
- Control Name
- Control Description
- Control Type
- Procedure Name

- Procedure Description
- Physical Evidence Produced

The query results are shown in a tabular format with data displayed for the above columns.

Business Process Summary report

This report shows the detailed view of a parent process. You can choose to view a specific number of levels in the hierarchy below the parent process. For example, you may wish to report on the Order to Cash process, its child processes, and grandchild processes.

Discoverer Workbook Name: AMW Control Reports

Folder Name: Business Process Summary

Seeded Query: This seeded query will retrieve the summary of a process with the attributes shown below.

Report parameters and search results

The report has the following default parameters:

- Parent Process Name

The default columns of the report are shown below:

- Parent Process
- Child Process
- Child Process Item Type

The query results are shown in a tabular format with data displayed for the above columns.

Process Organization Summary report

This report provides information on the organization to which a process is associated.

Discoverer Workbook Name: AMW Control Reports

Folder Name: Organization Summary

Seeded Query: This seeded query will retrieve details on the organization associated with a process.

Report parameters and search results

The report has the following default parameters:

- Process Name

The default columns of the report are shown below:

- Process Name
- Organization Name
- Process Owner
- Certification Status
- Approval Status

- Last Audit Status
- Last Audit Date
- Next Audit Date

The query results are shown in a tabular format with data displayed for the above columns.

Audit Procedures Summary report

This report provides details on audit procedures associated with a particular process, risk, or control.

Discoverer Workbook Name: AMW Control Reports

Folder Name: Audit Procedure Reports

Seeded Query: This seeded query will retrieve a summary of the audit procedures associated with a process.

Report parameters and search results

The report has the following default parameters:

- Process Name
- Risk Name
- Risk Description

The default columns of the report are shown below:

- Process Name
- Risk Name
- Risk Description
- Control Name
- Control Description
- Audit Procedure Name
- Audit Procedure Description
- Date Last Executed

The query results are shown in a tabular format with data displayed for the above columns.

Extensible Attributes

This chapter covers the following topics:

- Introduction
- Enabled Objects
- Setup of Extensible Attributes
- Recording Extensible Attributes

Introduction

Users interact with a variety of risk library objects while monitoring ongoing compliance using Oracle Internal Controls Manager. It is necessary and useful to capture and track additional and unique data associated with these objects. The application provides you with this ability in the form of Extensible Attributes.

These are user defined attributes that serve to capture additional information associated with risk library objects. Entries for these attributes can be validated against predefined value sets.

Consider the following examples, all of which relate to creating Extensible Attributes in a particular context:

- When dealing with risk objects, you may want to capture the attribute "Potential Damage" with pre-defined levels.
- When an audit procedure is created, you may want to interpolate an attribute "Level of complexity," again with pre-defined levels. You may also want to provide the originator with a text box to allow free text regarding this dimension.
- When you create a process, you may want to enter its "Jurisdiction."

Enabled Objects

Oracle Internal Controls Manager provides for extensible attributes linked to the following object groups:

- Risk Library processes
- Organization processes
- Risks
- Controls
- Audit Procedures

Note: You can also setup Extensible Attributes when creating Sign Off procedures with Audit Engagements. Refer to Sign Off procedures in Audit Engagements, page 8-9.

Attribute values are recorded during the course of evaluating and working with the above objects and can incorporate any aspect of firm execution in these areas.

Extensible Attributes and Classifications

Oracle Internal Controls Manager uses the "Classification" construct to distinguish the different sets of extensible attributes that can be associated with an object. When an object like an organization process is created with a particular classification, the application automatically logs it as having the extensible attributes associated with that classification and object group.

Consider the following example:

"Enter Orders" is an Organization Processes object with a classification "Ext Attr Org Type 1"

Home Financial Statements Audit Operations Segregation of Duties Organizations

Organizations > Organization: Vision Corporation > Process Hierarchy: Workbench: Vision Corporation > Process Details: Enter Orders, Vision Corporation

Process Details: Enter Orders, Vision Corporation

Printable Page Update Go

Classification: Ext Attr Org Type 1
Approval Status: Draft
Standard: N/A

Process Information Significant Controls Process Controls Audit Procedures Audit History People Enter

Process

| | | | |
|-------------------------|-------------|-----------------------|-----------------|
| Process Category | Routine | Process Type | |
| Control Type | | Classification Status | |
| Last Certification Date | | Last Audit Status | Materially Weak |
| Last Audit Date | 25 FEB 2005 | | |

Organization

| | | | |
|-------------------|-----------------------|----------------|--------------------|
| Organization Name | Vision Corporation | Category | US Operations |
| Type | Corporate Headquarter | Location | New York |
| Line of Business | PERSONAL COMPUTERS | OR Description | Personal Computers |

Process Significance

Process Significance Details

Element

Significance Details

Extensible Attributes "Govt Sponsor" and "Jurisdiction" can be associated with the "Enter Orders" process in the "Vision Corporation" organization.

Home Financial Statements Audit Operations Segregation of Duties Organizations

Organizations > Organization: Vision Corporation > Process Hierarchy: Workbench: Vision Corporation > Process Details: Enter Orders, Vision Corporation > Update Federal

Update Federal

Govt Sponsor Jurisdiction

Completely different Extensible Attributes, for example "Level of Complexity" and "Process Lifecycle Length" can be associated with "Organization Processes" for the classification "Ext Attr Org Type 2."

Note: It is important to note the following caveat: once a classification is linked to an object, the classification cannot be changed.

The implementation of Extensible Attributes in Oracle Internal Controls Manager is discussed in the following sections:

- Setup of Extensible Attributes
- Recording Extensible Attributes

Setup of Extensible Attributes

Before Extensible Attributes can be used in Oracle Internal Controls Manager, they must be set up as described in this section. Note that these setups are undertaken for a particular object group (like risks, controls, etc) and all Extensible Attributes associated with that group (for a particular classification value) will accordingly display the setups.

It is useful to remember the following order:

Object Group (for example Organization Process)

|

1 or more Classifications

|

1 or more Pages (for each Classification)

|

1 or more Attribute Groups (for each Page)

|

1 or more Attributes (for each Attribute Group)

Perform the following steps to define attributes and attach them to the objects for each object group:

1. Define Value Sets and Values
These need to be set up only if validation is needed for the new attributes.
2. Define Attribute Groups and Attributes. Associate Value Sets to Attributes.
3. Create Classifications for the object group and associate the Attribute Groups to them
4. Define Pages to display the Attribute Groups

1. Define Value Sets and Values

| Topic | Navigation Path |
|-------------------|---|
| Define Value Sets | Using the Super User (or equivalent) responsibility, click the Setup tab and then the Value Sets subtab. Drill down into the Value Sets hyperlink to create the Value Set. You will also define appropriate values from this window. |

2. Define Attribute Groups and Attributes. Associate Value Sets to Attributes.

It is important to remember that Attribute Groups are created and associated with particular object group like risks, controls, etc. Hence an Attribute Group created for risk objects is not available to control objects.

| Topic | Navigation Path |
|---|--|
| Define Attribute Groups and Attributes. | <p>Using the Super User (or equivalent) responsibility, click the Setup tab and then the Risk Library subtab. Select the Attributes hyperlink for the appropriate object group and then click the Create button.</p> <p>Once the basic information is entered, you can create attributes for the group. Each of the attributes created can be linked to a value set defined in step 1.</p> |

The following table provides further information on select fields in the Create Attribute Groups page.

| Name | Description |
|----------------|--|
| Multi-Row | <p>An attribute group can be multi-row or single-row. Multi-row attribute groups enable you to associate multiple sets of attribute values with the same object instance.</p> <p>For example, if "Exposure" was a multi-row attribute, then you can associate multiple "Exposure levels" with the attribute. For Single Row attribute groups, you can enter only one value for each attribute.</p> |
| View Privilege | <p>You can restrict access to the attributes in the attribute group to a specific role. Users must then have a view privilege for any object to which this attribute group is associated. You can thus narrow viewing privileges to meet the needs of your enterprise.</p> <p>Note: For more information, refer to the Oracle Advanced Product Catalog User Guide.</p> |
| Edit Privilege | <p>You can similarly restrict update capability on the attributes in the attribute group to a specific role.</p> <p>Note: For more information, refer to the Oracle Advanced Product Catalog User Guide.</p> |

Generate Database View button

Third-party systems integrators can easily generate a database view of existing attributes and attribute groups. These views are particularly useful when users wish to read the catalog data as they write code for integration with the Advanced Product Catalog product.

To generate database views, on the Search: Attribute Groups page, select the attribute groups for which you wish to generate the view and click Generate Database View.

3. Create Classifications for the Object Group and Associate the Attribute Groups to them

| Topic | Navigation Path |
|--|---|
| Create Classifications and associate Attribute Groups to the object classification | <p>Using the Super User (or equivalent) responsibility, click the Setup tab and then the Risk Library subtab.</p> <p>Select the Classification hyperlink associated with the object group for which attributes have been setup (described in point 2 above) and click the Create button.</p> <p>Once the classification is created, you can drill into its details to add the Attribute Group created in point 2 above.</p> |

4. Define Pages to display the Attribute Groups

| Topic | Navigation Path |
|----------------------|---|
| Finding Type details | <p>Drill into the appropriate Classification as described in 3. above and then click on the Pages subtab.</p> <p>Finally, click on the Create Page hyperlink and then the "Add Another Row" button to associate one or more Attribute Groups to the page.</p> |

Note: Creating Attributes and attaching them to Extensible Attributes uses functionality originally devised in the Oracle Product Lifecycle Management module.

If you need further information on creating Value Sets, Attribute Groups, and Attributes, refer to the following sections in the *Oracle Advanced Product Catalog Implementation Guide*:

- Chapter 4: Change Management Administration
- Chapter 7: Attributes and Function Administration

Recording Extensible Attributes

You can record extensible attributes in conjunction with any of the objects listed in the section Extensible Attribute Enabled Objects.

1. When creating/updating the object, enter the Classification.

The screenshot shows the Oracle Advanced Product Catalog Implementation Guide interface. The breadcrumb trail indicates the path: Organizations > Organization Sales 1004 > Process Details > Campaign to Cash Sales 1004 > Update Process: Campaign to Cash, Sales 1004. The form title is 'Update Process: Campaign to Cash, Sales 1004'. The process name is 'Campaign to Cash' and the version number is '2'. The 'Basic Information' tab is selected, showing fields for Process Type (Campaign), Category (Wholesale), and a dropdown for Classification. The 'Classification' dropdown is open, showing options like 'Ed All Org Type 1' and 'Complex Processes'.

Roles and Privileges in Oracle Internal Controls Manager

This chapter covers the following topics:

- Introduction to Security in Oracle Internal Controls Manager
- Data Security Details

Introduction to Security in Oracle Internal Controls Manager

Security in the application is implemented through both

- Function Security
- Data Security

Function Security

The Oracle E-Business Suite architecture often aggregates several related business functions into a single window. These functions take the form of menus, buttons, views, etc. Since all users should not have access to every business function in a screen or menu path, the architecture provides the ability to identify pieces of application logic as individual functions.

When part of an application's functionality is identified as a function, it can be secured (included or excluded from a responsibility). Application developers register functions when they develop the application windows. The E-Business Suite system administrator administers function security by creating responsibilities and menu structures that include or exclude particular functions. Oracle Internal Controls Manager provides function security in select windows of the application.

Note: For further details, refer to Function Security in Oracle Internal Controls Manager, page 16-1.

Data Security

In addition to function security, Oracle Internal Controls Manager enables a data security implementation as well.

Data security is at a lower level than function security in that users having access to the same function can view different data sets based on their data access rights. The concept is based on providing access privileges on instances of objects (like processes) to specific users or user groups.

Data secured objects (listed in the next section) in the Oracle Internal Controls Manager security architecture have privileges associated with them. For example, a user may be granted privileges like "View Process" and "Approve Process Changes" on a particular "Organization Process" object. This will allow the user to undertake these specific actions on this object to the exclusion of other organization processes.

Since the explicit granting of multiple privileges on each object to users can be overwhelming, the application provides for the granting of privileges to related objects in a cascading manner i.e. through "inherited roles." For example, if a user gets "Update" privileges on a parent process in an organization, then that user also automatically gets the same privileges on its subprocesses in that organization. The data security system also allows you to assign privileges to groups of users instead of assigning privileges to each user individually.

Note: To use Roles and Privileges in the application, the profile option AMW: Implement Data Security must be set to "Yes."

Roles

Privileges can be grouped together into an assigned "Role." Oracle Internal Controls Manager seeds a variety of roles corresponding to the object. Roles may be assigned to individuals and groups from the "People" tab in the details of the appropriate Oracle Internal Controls Manager object.

Data Security Details

Prerequisite

To enable roles and privileges on application objects, the profile option AMW: Implement Data Security must be set to "Yes" at the site level.

For a few select users, this profile value can be overridden by setting it to "No" at the user level. These users will have access to all objects and privileges and will effectively be "super user." All other users can only access objects based on their roles and privileges.

Oracle Internal Controls Manager super users grant different privileges to different users using the "People" subtab update button.

The application provides data security on the following objects:

1. Organizations
2. Organization Processes
3. Processes in the Risks Library
4. Audit Engagements

Roles and privileges on these objects are described in the following sections.

Organizations

| Topic | Navigation Path |
|---------------------------------|---|
| Implement Organization Security | Using the OICM Super User (or equivalent) responsibility, navigate to the Organizations tab. Drill into the details of the appropriate organization to access the People subtab. |

You can add and/or modify roles in this window.

Organizations

Update People

Indicates required field

Cancel Apply

Select People: Select

Select Role

| Select Role | Type | Name | Start Date | End Date |
|--|--------|----------------|-------------|----------|
| <input type="checkbox"/> Organization Manager | Person | Jonathan Smith | 15 Feb 2015 | |
| <input type="checkbox"/> Organization Details Viewer | Person | Jonathan Smith | 15 Feb 2015 | |
| <input checked="" type="checkbox"/> Organization Auditor | Person | Jonathan Smith | 15 May 2015 | |

Cancel Apply

Four roles are available to access organizations

1. Organization Change Approver
2. Organization Details Viewer
3. Organization Manager
4. Organization Auditor

The following table lists the privileges available to these roles:

| Privileges | Details | Organization Manager Role | Organization Change Approver Role | Organization Details Viewer Role | Organization Auditor |
|---|--|---------------------------------|--|--|-------------------------|
| View Organization Details | Get org in search result, view org details, view all subtabs | X | X | X | |
| Modify Organization Risks | Modify entity risk associations in an organization | X | | | |
| Modify Organization Controls | Modify entity control associations in an organization | X | | | |
| Modify Organization Attachments | Modify attachments to an organization | X | | | |
| Modify People | Give grant to people | X | | | |
| Modify Organization Audit Procedures | Modify entity AP in an organization | X | | | |
| Certify Organizations | NA | X | | | |
| Audit Organizations | NA | X | | | X |
| Approve Organization Changes | When you change a process in the organization, the person with this privilege gets to approve the change | X | X | | |

Notes

- The Organization Manager inherits the following roles on objects in the application:
 - Process Owner role on All Processes
 - Risk Viewer role, Control Viewer role, Audit Procedure Viewer role on the respective objects
- The Organization manager gets ownership on all organizations in the downward hierarchy of the organization

- The person who creates an organization automatically obtains the Organization Manager role
- The Organization Auditor role is granted to all users by default. However, only users with Internal Auditor responsibility will have appropriate access to organizations.

Organization Processes

| Topic | Navigation Path |
|---|--|
| Implement Organization Process Security | <p>Using the OICM Super User (or equivalent) responsibility, navigate to the Organizations tab and into the details of the appropriate organization.</p> <p>In this organization, drill down into the process being setup to access the People subtab.</p> |

Five roles are available to access organizations, and the following table lists the privileges available to these roles:

| Privileges | Details | Organization Process Owner | Organization Process Reviewer | Organization Process Change Approver | Organization Process Finance Owner | Organization Application Owner |
|---|--|----------------------------------|-------------------------------------|---|---|--------------------------------------|
| View Approved Process | View process in approved hierarchy. view approved process details. | X | X | X | X | X |
| Update Process | Go to latest hierarchy for any process, view details of process from latest hierarchy, update process button, update process attributes only | X | | X | X | X |
| Update process-risk association | Update process-risk association | X | | X | X | X |
| Update process- risk-control association | Update process-risk-control association | X | | X | X | X |

| Privileges | Details | Organization Process Owner | Organization Process Reviewer | Organization Process Change Approver | Organization Process Finance Owner | Organization Application Owner |
|--|---------------------------------------|----------------------------------|-------------------------------------|---|---|--------------------------------------|
| Update key account association | Update key account association | X | | X | X | X |
| Update objective association | Update objective association | X | | X | X | X |
| Attach audit procedures from control details or vice versa | Audit Procedure Addition to a Process | X | | X | X | X |
| Add people to Process | Grant Role to People | X | | X | X | X |
| Approve Process Changes | Approve Process Changes | X | | X | X | X |
| Certify Organization Process | Certify Organization process | x | | | X | X |

Notes:

- All five roles can view details of risks, controls, and audit procedures associated to the process
- If a user is granted a role on a process, then that user is also granted the same role on all its children
- The user who creates an organization process (associates the process to the organization), automatically gets the "Organization Process Owner" role on that process

Risk Library Processes

| Topic | Navigation Path |
|--|--|
| Implement Security on Risk Library Processes | Using the OICM Super User (or equivalent) responsibility, navigate to the Risk Library tab and the Processes subtab. Drill into the details of the appropriate process to access the People subtab. |

Five roles are available to access risk library process objects and the following table lists the privileges available to those roles:

| Privileges | Details | Risk Library Process Owner | Risk Library Process Reviewer | Risk Library Process Change Approver | Risk Library Process Finance Owner | Risk Library Process Application Owner |
|--|--|----------------------------|-------------------------------|--------------------------------------|------------------------------------|--|
| View Approved Process | View process in approved hierarchy. view approved process details. | X | X | X | X | X |
| Update Process | Go to latest hierarchy for any process, view details of process from latest hierarchy, update process button, update process attributes only | X | | X | X | X |
| Update process-risk association | Update process-risk association | X | | X | X | X |
| Update process-risk-control association | Update process-risk control association | X | | X | X | X |
| Update key account association | Update key account association | X | | X | X | X |
| Update objective association | Update objective association | X | | X | X | X |
| Attach audit procedures from control details or vice versa | Audit Procedure Addition to a Process | X | | X | X | X |
| Add people to Process | Grant Role to People | X | | X | X | X |
| Approve Process Changes | Approve Process Changes | X | | X | X | X |

Notes:

- All five roles can view details of risks, controls, and audit procedures associated to the process
- If a user is granted a role on a process, then that user is also granted the same role on all its children
- The user who creates a risk library process, automatically gets the "Process Owner" role on that process.

Audit Engagements

| Topic | Navigation Path |
|--|--|
| Implement Security on Risk Library Processes | Using the Internal Auditor (or equivalent) responsibility, navigate to the Audit Operations tab and the Engagements subtab. Drill into the details of the appropriate Audit Engagement to access the People subtab. |

Five roles are available to access audit engagement objects and the following table lists the privileges available to those roles:

| Privileges | Details | Engagement Manager | Engagement Approver | Engagement Reviewer | Engagement Auditor |
|---|---|--------------------|---------------------|---------------------|--------------------|
| View Scope | View Scope | X | X | x | x |
| Add / Remove Subsidiary / LOB / Organization, Manage Included Processes | Update Scope | x | | | |
| View Audit Tasks | View Audit Tasks | x | x | x | x |
| Update Task Info | Add / Copy / Move Audit Procedures to Task, Remove Audit Procedures from Task, Create / Update Audit Procedures in engagement | x | | | x |
| View Audit Procedures Execution Details | View Audit Procedures Execution Details (and the associated controls) | x | x | x | x |

| Privileges | Details | Engagement Manager | Engagement Approver | Engagement Reviewer | Engagement Auditor |
|--------------------------|--|--------------------|---------------------|---------------------|--------------------|
| Execute Audit Procedures | Execute Audit Procedures and Audit Procedures step, Evaluate Control in Audit Procedures context | x | | | x |
| View Controls | View Controls (and the associated Risks and Audit Procedures) | x | x | x | x |
| Evaluate Controls | Evaluate Controls | x | | | x |
| View Risks | View Risks (and the associated Controls and Processes) | x | x | x | x |
| Evaluate Risks | Evaluate Risks | x | | | x |
| View Processes | View Processes | x | x | x | x |
| Evaluate Processes | Evaluate Processes | x | | | x |
| View Organizations | View Organizations | x | x | x | x |
| Evaluate Organizations | Evaluate Organizations | x | | | x |
| View Findings | View Findings (for Organization / Process / Risk / Control / AP) | x | x | x | x |
| Update Findings | Update Findings (for Organization / Process / Risk / Control / Audit Procedures) | x | | | x |
| View Persons | View Persons | x | x | x | x |
| Update Persons | Update Persons | x | | | |

| Privileges | Details | Engagement Manager | Engagement Approver | Engagement Reviewer | Engagement Auditor |
|----------------------------------|----------------------------------|-----------------------|------------------------|------------------------|-----------------------|
| Sign Off | Sign Off | | x | | |
| View Audit Objectives | View Audit Objectives | x | x | x | x |
| Update Audit Objectives | Update Audit Objectives | x | | | |
| View Engagement settings | View Engagement settings | x | x | x | x |
| Update Engagement settings | Update Engagement settings | x | | | |

Function Security in Oracle Internal Controls Manager

This chapter covers the following topics:

- Introduction
- Processes in Oracle Internal Controls Manager
- Controls in Oracle Internal Controls Manager
- Audit Procedures in Oracle Internal Controls Manager
- Risks in Oracle Internal Controls Manager
- Audit Project Evaluations in Oracle Internal Controls Manager
- Process Certifications in Oracle Internal Controls Manager
- Financial Statement Certifications in Oracle Internal Controls Manager
- Issue Management in Oracle Internal Controls Manager

Introduction

The Oracle E-Business Suite architecture often aggregates several related business functions into a single window. Since all users should not have access to every business function in a screen or menu path, the architecture provides the ability to identify pieces of application logic as functions.

When part of an application's functionality is identified as a function, it can be secured (included or excluded from a responsibility). Application developers register functions when they develop the application windows. The E-Business Suite system administrator administers function security by creating responsibilities that include or exclude particular functions.

Oracle Internal Controls Manager provides function security in select windows of the application.

Note: For a thorough introduction to function security in the Oracle E-Business Suite, refer to the *Oracle Applications System Administrator's Guide*.

Note: Also refer to Roles and Privileges in Oracle Internal Controls Manager, page 15-1

The following tables provide detailed information on the security functions available within the various domains of Oracle Internal Controls Manager.

Processes in Oracle Internal Controls Manager

| User Function name | Function Code Value | Description | Menu Path to Access the Function |
|----------------------------|----------------------------|------------------------|---|
| AMW Process Details | AMW_PROCESS_DETAILS | View Process Details | <p>Using the Internal Controls Manager Super User (or equivalent) responsibility, click the Risk Library tab and then the Processes subtab. The function corresponds to the detailed view of a process.</p> <p>If you log in using a Business Process Owner responsibility, you can also access process details via the Organizations tab.</p> |
| AMW Allow Process Creation | AMW_ALLOW_PROCESS_CREATION | Allow Process Creation | <p>Under the Risk Library > Processes subtab, the function corresponds to the Convert Tutor Document button. However, if the function is not available to a responsibility, the application will also prevent the user from using WebAdi to create processes.</p> <p>Note that creating and importing process from Oracle Workflow must be secured in the workflow module.</p> |

| User Function name | Function Code Value | Description | Menu Path to Access the Function |
|------------------------------------|--------------------------|---|---|
| AMW Allow Process Update | AMW_ALLOW_PROCESS_UPDATE | Allow Process Update | Using an appropriate responsibility, click the Risk Library tab and drill down into the details of the applicable process. The function corresponds to the Update button in this view. It also controls the association and disassociation of processes in an Organization context. |
| AMW Secure Process Synchronization | AMW_PROCESS_SYNC_ALLOW | Enable Secure Process Synchronization privilege | Using an appropriate responsibility, click the Risk Library tab and drill down into the details of the applicable process. The function corresponds to the Synchronize button in this view. |

Controls in Oracle Internal Controls Manager

| User Function name | Function Code Value | Description | Menu Path to Access the Function |
|--------------------------|--------------------------|--|--|
| AMW Create/Update/Delete | AMW_CR_UPD_DEL_CTRL_RESP | Allow create, update and delete privilege for controls | Using the Internal Controls Manager Super User (or equivalent) responsibility, click the Risk Library tab and then the Controls subtab. The function corresponds to the create button as well as the update and delete icons. |
| AMW Associate Control | AMW_ASSOC_CTRL | Enable associate control privilege | Under the Risk Library > Controls subtab, drill into the appropriate Control and then click on the Risks hyperlink. The function corresponds to the Add button in both Risks AND Audit Procedures sections. |

Audit Procedures in Oracle Internal Controls Manager

| User Function name | Function Code Value | Description | Menu Path to Access the Function |
|----------------------------|-----------------------|-------------------------------------|--|
| AMW Create Procedure Page | AMW_CREATE_PROCEDURE | Enable creation of audit procedures | Using the Internal Controls Manager Super User (or equivalent) responsibility, click the Risk Library tab and then the Audit Procedures subtab. The function corresponds to the create button in this view. |
| AMW Procedure Details Page | AMW_PROCEDURE_DETAILS | View audit procedures | The function corresponds to the detailed view of an audit procedure. |

Risks in Oracle Internal Controls Manager

| User Function name | Function Code Value | Description | Menu Path to Access the Function |
|-------------------------------------|-----------------------|--|--|
| AMW Allow Create/Update Risk | AMW_RISK_CREATE_ALLOW | Enable creation of Risks | Using the Internal Controls Manager Super User (or equivalent) responsibility, click the Risk Library tab and then the Risks subtab. The function corresponds to the create button in this view. |
| AMW Allow Associate Risk to Process | AMW_RISK_ASSOC_ALLOW | Enable association of risks to process | In the Risk Library, drill down under the Risks subtab to the detailed view of a Risk. Then click on the Processes hyperlink. The function corresponds to the Add button in this view (used to associate the risk to a process). |

Audit Project Evaluations in Oracle Internal Controls Manager

| User Function name | Function Code Value | Description | Menu Path to Access the Function |
|---------------------------------------|--------------------------------|---|--|
| AMW Opinions Evaluate Organization | AMW_OPINIONS_ EVALUATE_ORG | Evaluate an Organization in the Project context | Using the Internal Auditor (or equivalent) responsibility, click the Audits tab and then the Projects subtab. Drilldown into the appropriate project and select the Organizations and Processes hyperlink. The function corresponds to the Evaluate icon for the relevant organization. |
| AMW Opinions Evaluate Process | AMW_OPINIONS_ EVALUATE_PROC | Evaluate a Process in the Project context | Under the Audits > Projects subtab, drill down into the appropriate project and select the Organizations and Processes hyperlink. The function corresponds to the Evaluate icon for the relevant process. |
| AMW Opinions Evaluate Risk | AMW_OPINIONS_ EVALUATE_RISK | Evaluate a Risk in the Project context | Under the Audits > Projects subtab, drill down into the appropriate project and select the Risks hyperlink. The function corresponds to the Evaluate icon for the relevant risk. |

| User Function name | Function Code Value | Description | Menu Path to Access the Function |
|--|---------------------------------|---|--|
| AMW Opinions Evaluate Control | AMW_OPINIONS_ EVALUATE_CTRL | Evaluate a Control in the Project context | Under the Audits > Projects subtab, drill down into the appropriate project and select the Controls hyperlink. The function corresponds to the Evaluate icon for the relevant control. |
| AMW Opinions Evaluate Audit Procedure Control | AMW_OPINIONS_ EVALUATE_APCTR | Evaluate a Control in the Audit Procedure context | Under the Audits > Projects subtab, drill down into the appropriate project and click the Audit Tasks hyperlink. Next drill down into a task and then click the Current Status hyperlink associated with a procedure. Finally, click on the Control Evaluations link. The function corresponds to the Update icon within the body of the table. |

Process Certifications in Oracle Internal Controls Manager

| User Function name | Function Code Value | Description | Menu Path to Access the Function |
|---------------------------------|--|--|--|
| Amw Enable Global Process Owner | AMW_ENABLE_ GLOBALPROCESS_ OWNER | Enables global process owner access privilege i.e. the ability to see all processes. | N/A |
| AMW Opinions Certify Process | AMW_OPINIONS_ CERTIFY_PROC | Enables process certification privilege | Using a Business Process Owner (or equivalent) responsibility, click the Business Process tab and then the Certifications subtab. Drill into a Certification to access a summary page. The function corresponds to the Certify icon in this view. |

Note: To create or update a process certification in the Certification Summary page, BOTH the following security functions must be enabled for the user.

- AMW_ENABLE_GLOBALPROCESS_OWNER

- AMW_OPINIONS_CERTIFY_PROC

The "Send Reminder" button and "Certify" icon will not be displayed if the user does not have the AMW_OPINIONS_CERTIFY_PROC.

Financial Statement Certifications in Oracle Internal Controls Manager

| User function name | Function Code Value | Description | Menu Path to Access the Function |
|---|--------------------------------|--|---|
| AMW Financial Statement Certification Build | AMW_FINSTMT_CERT_BUILD | Create/Update a Financial Statement Certification | Using the Signing Officer or equivalent responsibility, click the Financial Statements tab and then the Certifications subtab. The function correspond to the Create button as well as the Update button in the detailed view. |
| AMW Opinions Evaluate Financial Item | AMW_OPINIONS_EVALUATE_FIN_ITEM | Evaluate a Financial Item in the Financial Statement Certification context | In the Financial Statement > Certifications subtab, drill into the details of a Certification and then click the Financial Items hyperlink. The function corresponds to the Evaluate icon for the Financial Item. |
| AMW Certify Financial Statement | AMW_CERTIFY_FIN_STMT | Certify a Financial Statement in the Financial Statement Certification context | In the Financial Statement > Certifications subtab, drill into the details of a Certification. The function corresponds to the Update button under the General tab (Certification Result). |

Issue Management in Oracle Internal Controls Manager

| User function name | Function Code Value | Description | Menu Path to Access the Function |
|--------------------------------|-----------------------|--|--|
| AMW Create Findings | AMW_CREATE_FINDINGS | Enable the creation of Findings | Findings can be entered in multiple places. Refer to the section Recording Findings in Oracle Internal Controls Manager, page 12-9. The function corresponds to the Create button in these views. |
| AMW Create Issues | AMW_CREATE_ISSUES | Enable the creation of Issues | Using a Business Process Owner (or equivalent) responsibility, click the Business Process tab and then the Certifications subtab. Drill into a Certification to access a summary page and then click on the Issues subtab. The function corresponds to the Create button in this view. |
| AMW Create Correction Requests | AMW_CREATE_CORRECTREQ | Enable the creation of Correction Requests | Using the Internal Auditor (or equivalent) responsibility, click the Audits tab and then the Segregation of Duties Violations subtab. The window shows a detailed listing of violations. Drill down into the Correction Request for a particular constraint violation. The function corresponds to the Create button in this view. Alternatively, you may drilldown into a violation and then click the Correction Requests hyperlink. The function corresponds to the Create button in this view. |

Introduction to Application Controls Monitoring

This chapter covers the following topics:

- Introduction
- Introduction to Application Controls Monitoring and Governance
- Overview of the Application Controls Monitoring feature
- IT Audit Execution

Introduction

This chapter provides a broad overview of the Application Controls Monitoring domain and the solution provided by Oracle Internal Controls Manager..

Introduction to Application Controls Monitoring and Governance

The accuracy and reliability of a firm's business processes and financial reporting are to a great extent dependent on the reliability and functioning of its IT systems and control environment. In the post Sarbanes-Oxley world, companies are increasingly dependent on automatic application controls to ensure compliance with regulatory and company policies. IT is now tasked with ensuring that these controls effectively support the firm's objectives.

To meet the ongoing demands of assessing the IT control environment and minimize the cost of compliance, IT departments need an automated approach for monitoring and testing IT controls. To help them meet these new responsibilities, many IT organizations have adopted the "Control Objectives for Information and related Technology" (CobiT) framework for managing IT related risks and controls.

Note: While both COSO and CobiT address controls in the enterprise, CobiT focuses mainly on IT controls. This distinction translates into differences in the scope of each control framework.

As a result, while COSO control objectives are targeted towards reliable financial reporting and compliance with regulations, CobiT's role targets quality and security requirements.

IT Audits and the CobiT Framework

At its heart, the CobiT framework recognizes a process basis in the deployment and management of IT resources. It correspondingly addresses IT Audits through this process centric lens.

CobiT identifies 34 information technology processes grouped into four domains.

- Planning and Organization
- Acquisition and Implementation
- Delivery and Support
- Monitoring.

This classification presents a firm's IT activities in a manageable and logical structure.

All processes are subject to risk. Due to the pervasive nature of IT in most organizations, the management of IT related processes and risks is a critical part of enterprise risk management. IT Auditors therefore identify the risks associated with those process and the possible effect they might have on the enterprise.

IT controls (control procedures within a particular IT activity) are designed to mitigate the risks from execution of the IT related processes. The CobiT framework therefore continues with a set of 34 high level control objectives, one for each of the IT processes. It also furnishes detailed control objectives and audit guidelines to assess the IT processes. By addressing these control objectives, firms can ensure that an adequate control system oversees the IT environment.

Overview of the Application Controls Monitoring feature

The Application Controls Monitoring feature enables companies to effectively and efficiently manage their IT environment by monitoring IT controls within the Oracle E-Business Suite. The application supports a number of high level control objectives within the CobiT framework such as maintaining application software, managing changes, ensuring systems security, and managing configuration.

The Application Controls Monitoring feature is a constituent in the Oracle Internal Controls Manager (OICM) product.

Application Controls in the Oracle E-Business Suite

The Oracle E-Business Suite offers a comprehensive set of automated application controls in the form of setup parameters. These application controls are critical to the overall control environment because any changes to them can have an adverse effect on the organization's processes including those that influence the reliability and integrity of financial reporting.

Examples of Application Controls (Setup Parameters):

1. Setup accounts are a good example of these parameters. Several applications require that certain accounts be seeded as part of the implementation of the application.

Consider the Realized Gain and Loss Accounts in Oracle Payables. These accounts must be identified before the application can be used to capture gains and losses on payables transactions. An erroneous change in these accounts could lead to their misclassification and creates the risk of materially understating / overstating gains and losses in financial statements.

2. As another example, consider the Purchasing setup option "Price Tolerance Percentage." A change in this percentage must be visible to process owners as it could affect mandated purchasing guidelines.

Since changes to setup parameters affect the control environment encompassing the firm's business processes, these changes constitute a significant risk to the organization. In addition, the audit trail of application change activity is of increased importance in the light of regulatory requirements.

It is therefore essential that setup changes be monitored and reported. Within the Oracle E-Business Suite, this will involve tracking essential application controls in applications including (but not limited to) Payables, Receivables, Purchasing, and Inventory. Through these applications, Application Controls Monitoring can also track application controls in business flows like Procure to Pay and Order to Cash.

Application Controls Management using the OICM Application Controls Monitoring feature

Application Controls Monitoring enables IT managers and IT auditors to track changes to application controls in several modules within the Oracle E-Business Suite.

Note: For a detailed listing of the specific Applications and Setup Parameters that can be audited for changes, refer to Seeded Setup Groups and Parameters, page 21-1.

Application Controls Monitoring uses an intuitive workbench to provide features and benefits like the following:

Detailed Information regarding Setup Changes

Any change that is made to an application control can now be monitored and reported on. Application Controls Monitoring also enables the capture and reporting of related information like who made the change, when it was undertaken and the current and prior value of the setup data. You can also view a detailed change history for the application control.

Multiple Search Criteria

IT managers can search for changes in application controls using different criteria like application, organization, date range or user. Application Controls Monitoring would then show changes just for that specific entity or period.

In addition, the search criteria can be refined to look for changes in a particular "Reporting Group." A Reporting Group is a user-defined group of setup parameters. For example, the owner of the Procure to Pay process can setup a Reporting Group called "Procure to Pay RG" and track all the setup parameters that are important for this Procure to Pay process. These parameters can then be tracked and analyzed as a group on an ongoing basis.

Similarly, you can also search for changes by date range or GL time period. This is an extremely useful feature as you can now track the changes made to application controls during a specific period like a fiscal quarter or year. SOX rules in the USA require firms to disclose any material changes to internal controls that have made in a reporting period.

Finally, in the case of suspected fraud or erroneous changes to application setups, Application Controls Monitoring also enables an IT manager to identify all

changes made by a particular user. Note that all application control changes identify the user who executed the change and when the control was altered.

Track Setup Changes Across Multiple Instances

With Application Controls Monitoring, IT managers can continuously monitor changes to application controls across multiple application instances. This feature is particularly useful in troubleshooting configuration problems as the application allows you to compare controls across instances as well as against user defined standards (see Recommended Control Settings below).

Seeding and Comparison with Recommended Control Settings

Recommended values can be set up in Application Controls Monitoring. This content is typically from audit and risk assurance firms who have repositories of recommended control setting values predicated on industry and firm size.

You can then view and report on the comparison between actual and recommended values for setup data. This information can provide evidence that the intended application controls are in place or whether they need to be investigated further.

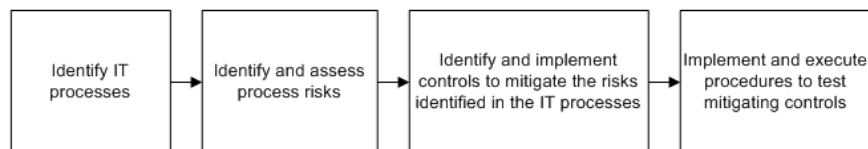
Out-of-the-Box Monitoring

Application Controls Monitoring delivers setup parameters for all key financial modules in the Oracle E-Business Suite, enabling out-of-the-box monitoring of these application controls.

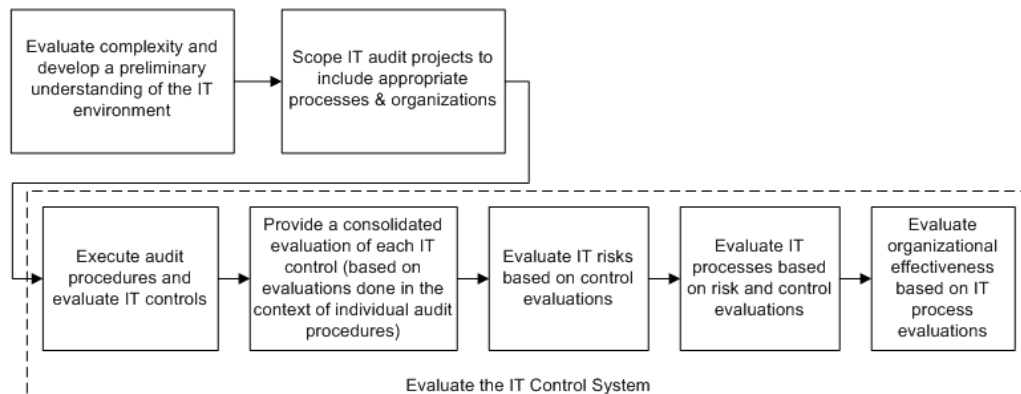
IT Audit Execution

The IT audit domain recognizes the roles of IT managers and auditors in conducting IT Audits. Because of a degree of overlap between the roles, up front and effective work by an IT manager can significantly alleviate the costs of a typical IT audit.

IT Manager



IT Auditor



The following sections provide a high level overview of the tasks of a typical IT Auditor.

Evaluate the Complexity of IT Processes

The degree of complexity and a preliminary understanding of the firm's IT system influences the scope of work an IT auditor must undertake. The pervasive presence of computer technology in today's enterprise requires evaluating IT systems to assess the degree of reliability of those systems.

As noted earlier, the CobiT Framework recognizes a process basis to the architecture of IT resources. The framework references most IT controls in the context of business processes.

Scope the IT Audit Project

The scope of the IT project determines which entities and processes are included in the project and therefore defines the context in which audit procedures are executed. The scope provides boundaries to the execution of the IT audit. Once the scope is resolved, an auditor can finalize the audit procedures that comprise the audit project.

The scoping task involves selecting the entities that will be included in the audit. Entities typically include the companies, lines of businesses within those companies, and finally the processes from organizations belonging to the selected companies and lines of businesses.

Evaluate the IT Control System

IT audits are generally based on a risk control framework. Auditors identify the risks associated with each business process and the possible effect they might have on the enterprise. Information related risks are typically classified into the following:

- Business risk: For example, the overall risk associated with acquiring new hardware and software.
- Audit Risk: The risk that an incorrect audit opinion is made.
- Security Risk: Risks associated with data access and integrity.
- Continuity Risks: Risks associated with the system's availability, backup and successful recovery.

Controls are identified and implemented to mitigate these risks. Audit procedures will test the IT controls to provide the degree of reliability on the firm's IT systems i.e. risks are assessed based on control evaluations.

IT processes are subsequently evaluated based on assessments of these risks and mitigating controls. The CobiT framework provides audit guidelines to enable the review of IT processes against the recommended detailed control objectives. IT auditors are also increasingly involved with substantive testing of the data in financial audits.

Finally, organizational entities are evaluated based on the evaluation of processes within them and an opinion of the IT system is rendered.

Application Controls Monitoring in the Audit Cycle

IT auditors conduct risk based audits to test the effectiveness of controls over IT processes. The results of the audit form a basis upon which auditors can attest that internal controls are functioning as intended. IT audits are best managed as projects. The

IT audit project represents a compilation of audit assignments for the IT system and becomes the central repository of information on the audit.

Application Controls Monitoring is not a tool to track the actual flow/audit of IT processes in the enterprise. The planning and execution of IT audit projects is best undertaken in an environment setup by the Oracle Internal Controls Manager application. Modelling IT audit execution within Oracle Internal Controls Manager is similar to how all risk based audits are executed.

Note: For detailed information on the setup, scoping, and execution of projects (IT or any audit project) in Oracle Internal Controls Manager, refer to Audit Engagements, page 8-1.

Within this larger context, Application Controls Monitoring can address IT Process risk in all four domains of the CobiT framework. The Application Controls Management feature directly mitigates this process risk through managing changes in application software, ensuring systems security, and managing configurations.

An IT manager can use Application Controls Monitoring in the implementation of controls on setup changes while IT auditors can use the module to assess IT risks.

Setup of Application Controls Management

This chapter covers the following topics:

- Introduction
- Definitions
- Application Controls Monitoring Architecture
- Setting Up Application Controls Management
- Note on Processing Business Events

Introduction

Before Application Controls Monitoring can be used to report on changes in application controls, it must be implemented appropriately.

This chapter provides all the information you need to define and setup the Application Controls Monitoring environment.

Definitions

The following definitions are important in understanding the architecture of the Application Controls Monitoring feature:

Source Tables

These are Oracle Applications tables that are used to store setup data. FINANCIALS_SYSTEM_PARAMS_ALL, GI_SETS_OF_BOOKS, AND PO_SYSTEM_PARAMETERS_ALL are examples of Source Tables. Application Controls Monitoring application captures and reports on the changes to data in these tables.

Note: For a complete and detailed listing of the Applications and Source Tables that are applicable to the Application Controls Monitoring feature, refer to Seeded Setup Groups and Parameters, page 21-1.

Shadow Tables

When the concurrent program "Audit Trail Update Tables" is run, Shadow Tables corresponding to all Source Tables are automatically created in the same Oracle ID as the Source Tables.

Shadow Tables contain primarily the Source Table columns to be audited. However, all columns in a Shadow Table are unconstrained regardless of their status in the original Source Table that is being audited. Shadow Tables also contain certain special auditing columns like Username and Timestamp columns.

Note: For detailed information on Shadow Tables, refer to the *Oracle Applications System Administrator's Guide*.

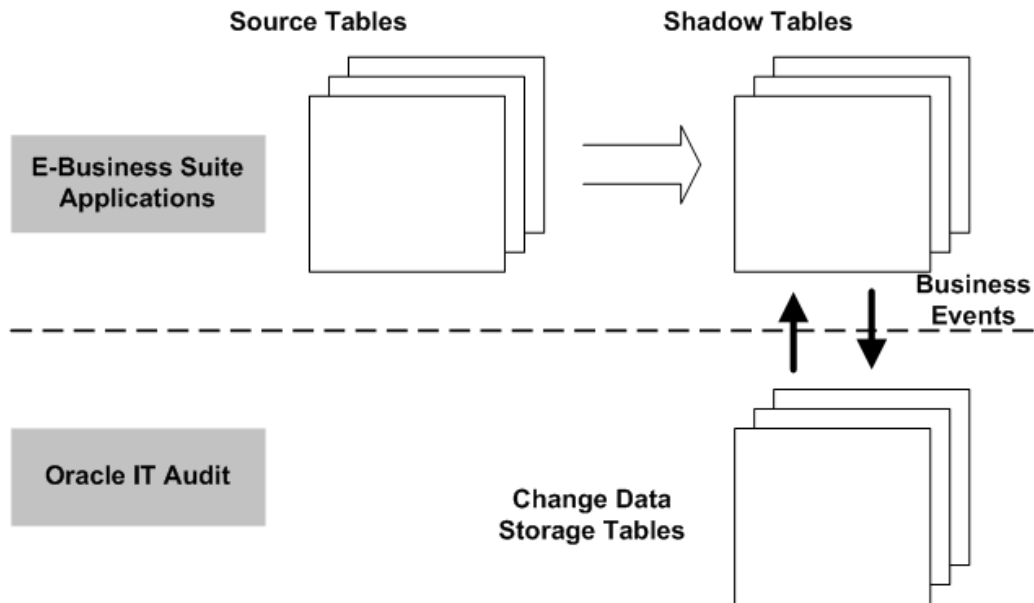
Change Data

Change Data pertains to data changes in a Source table. It includes the actual values that were changed, the time when it was changed, and who made the change. For update operations, change data will include the old and new values of columns updated.

Application Controls Monitoring Architecture

The Application Controls Monitoring feature exchanges data with Oracle E-Business suite applications as follows: When setup parameters change, the Setup Change Data is instantly recorded in Shadow Tables and asynchronously transferred to Change Data Storage Tables. The transfer is done using business events that are raised when the audit data is inserted in the Shadow Tables.

Note that while Source and Shadow Tables belong to the owning application, Change Data Storage Tables reside in the Oracle Internal Controls Manager schema. The following diagram depicts this mechanism for the capture and storage of Change Data.



Processing Business Events on Shadow Tables

As noted above, business events are raised whenever information is inserted in the Shadow Tables. These events are then placed on an event queue and subsequently processed in the same order when the Workflow Agent Listener picks them up.

Note: For more information on ensuring that all applicable events pertaining to setup changes are processed, refer to the Note on Processing Business Events, page 18-11.

Setting Up Application Controls Management

The following steps must be undertaken to set up Application Controls Monitoring:

- Implement Prerequisite Steps
- Review Setup Groups and Setup Parameters
- Define Reporting Groups
- Import Setup data from Remote Application Instances

Prerequisites

A successful implementation of Application Controls Monitoring requires the following prerequisites:

Prerequisite 1

Run the concurrent program "AuditTrail Update Tables." This concurrent program creates triggers and Shadow tables for each Source table in the audit trail group. The Shadow Tables created will have their name in the following format: "<source table name>_a."

Prerequisite 2

The profile option Audit Trail: Activate needs to be enabled at the site level. This option enables the logging of data within Shadow Tables.

Prerequisite 3

The concurrent program to enable setup tracking changes is called "ITA Enable Setup Change Tracking." This program should be run once as a post install step after the "Audit Trail Update Tables" concurrent program completes successfully.

Setup Groups

A Setup Group is an Application Controls Monitoring entity that maps to a Source Table in Oracle Applications.

| Topic | Navigation Path |
|--|--|
| Viewing seeded Setup Groups in Application Controls Monitoring | Using the IT Auditor (or equivalent) responsibility, click the Setup tab and then the Setup Groups subtab [Setup Groups Window]. |

Setup Groups represent the source objects that will be audited by Application Controls Monitoring and are currently seeded by Oracle.

Simple Search

[Advanced Search](#)

Setup Group Name

| <div> Previous <div>1-10</div> Next 10 </div> | | | |
|---|------------------|------------------------------|------------------------|
| Setup Group | Application | Table | Organization Type |
| Cash Parameters | Cash Management | CE_SYSTEM_PARAMETERS_ALL | Operating Unit |
| Financials Options | Payables | FINANCIALS_SYSTEM_PARAMS_ALL | Operating Unit |
| Inventory Parameters | Inventory | MTL_PARAMETERS | Inventory Organization |
| Invoice Tolerances | Payables | AP_TOLERANCES_ALL | Operating Unit |
| Order Entry Parameters | Order Management | OE_SYSTEM_PARAMETERS_ALL | Operating Unit |
| Payables Options | Payables | AP_SYSTEM_PARAMETERS_ALL | Operating Unit |
| Purchasing Options | Purchasing | PO_SYSTEM_PARAMETERS_ALL | Operating Unit |
| Receivables Options | Receivables | AR_SYSTEM_PARAMETERS_ALL | Operating Unit |
| Receiving Options | Purchasing | RCV_PARAMETERS | Inventory Organization |
| Set of Books | General Ledger | GL_SETS_OF_BOOKS | Set of Books |

Application Controls

Application Controls: User > Setup Group: Purchasing Options >

Update Setup Group: Purchasing Options

* Indicates required field

* Setup Group Name

Application **Purchasing**

Table **PO_SYSTEM_PARAMETERS_ALL**

| | |
|-------------------|----------------|
| Context Column | ORG_ID |
| Organization Type | OPERATING_UNIT |

Cancel Apply

Apply

18-4 Oracle Internal Controls Manager Implementation Guide

| Field | Description | Accessibility Level |
|-------------------|---|---------------------|
| Organization Type | <p>Setup tables that are supported by Application Controls Monitoring contain setup data at a particular organization level like operating unit, set of books, or inventory organization.</p> <p>The Organization Type represents the organization level that the setup group is associated with. For example the Setup Group Purchasing Options contains all its parameter values at the operating unit level.</p> | Not updateable |
| Context Column | The Context Column denotes internally which column in the Source table contains information pertaining to the organization. | Not updateable |

Note: For a detailed listing of all seeded Setup Groups applicable to Application Controls Monitoring, refer to Seeded Setup Groups and Parameters, page 21-1.

Setup Parameters

Each Setup Group can have multiple Setup Parameters. Setup Parameters map to specific columns in a Source Table. These are the columns which need to be audited for changes and hence the primary items of interest in Application Controls Monitoring.

| Topic | Navigation Path |
|----------------------------|--|
| Accessing Setup Parameters | <p>Using the IT Auditor (or equivalent) responsibility, click the Setup tab and then the Setup Groups tab [Setup Groups Window].</p> <p>Drill down into a particular Setup Group to view its Setup Parameters.</p> |


in a "comparison dashboard" are based on the setup parameter's divergence from its recommended value.

| Application Controls Setup | | | | | | | | | |
|--|----------------------|--|----------------|-------------------|-------------|-------|----------------------|----------------------|-----------------|
| Reporting Group Application User Instance | | | | | | | | | |
| Browse Application Controls Changes by Reporting Group | | | | | | | | | |
| * Indicates required field | | | | | | | | | |
| ▶ Show Search Criteria | | | | | | | | | |
| Details | Setup Group | Parameter | Organization | | Value | | | Last Updated On | Last Updated By |
| | | | Type | Name | Recommended | Prior | Current | | |
| ▶ Show | AR System Parameters | Allow Override | Operating Unit | Vision Operations | | | Y | 22-Dec-2004 21:10:54 | LEASE |
| ▶ Show | AR System Parameters | AutoCash Rule Set | Operating Unit | Vision Operations | | | Standard | 22-Dec-2004 21:10:54 | LEASE |
| ▶ Show | AR System Parameters | Finance Charge Activity | Operating Unit | Vision Operations | | | | 22-Dec-2004 21:10:54 | LEASE |
| ▶ Show | AR System Parameters | Tax Account | Operating Unit | Vision Operations | | | 01-000-2520-0000-000 | 22-Dec-2004 21:10:54 | LEASE |
| ▶ Show | AR System Parameters | Days in Days Sales Outstanding Calculation | Operating Unit | Vision Operations | 300 | ⊗ 365 | ⊗ 360 | 21-Jan-2005 09:50:29 | AUDITOR |

In the dashboard view, if the current value of a particular Setup Parameter does not equal its recommended value, Application Controls Monitoring displays a red cross next to that value. With this flag, a quick scan of the dashboard can alert a user to the Setup Parameter and instance that must be investigated.

To enter a Recommended Value

| Topic | Navigation Path |
|---|--|
| Enter Recommended Values for Setup Parameters | <p>Using the IT Auditor (or equivalent) responsibility, click the Setup tab and then the Setup Groups tab [Setup Groups Window].</p> <p>Drill down into a particular Setup Group to view its Setup Parameters and subsequently drill down into the Setup Parameter in question.</p> <p>Finally, click on the Recommended Values subtab to enter the appropriate value.</p> |

| Application Controls Setup | |
|--|---|
| Setup Groups Reporting Groups Instances | |
| Setup: Setup Groups > Setup Group: Financials Options > Parameter: Payment Terms > | |
| Create Recommended Value | |
| * Indicates required field | |
| Organization | <input type="text"/>  <input type="checkbox"/> Default Value |
| * Recommended Value | <input type="text"/> |
| <input type="button" value="Cancel"/> <input type="button" value="Apply"/> | |

Specify the recommended value by organization. When you specify a recommended value, you may choose to mark it as a default value. If specified as a default, then the value applies in all organizations except those in which the Setup Parameter already has a value.

Note: Entering a recommended value without specifying the organization is equivalent to creating it as a default value.

Entering a recommended value in a particular organization overrides the default value. To change a recommended value in a specific organization, you are required to update the value as opposed to entering a new value for that org.

History

While setting up recommended values for Setup Parameters you may view a history of changes to these values for each organization in the form of the following:

- Current recommended value
- Current value
- Immediately prior value

Setup Groups | Reporting Groups | Instances

Setup: Setup Groups > Setup Group: Financials Options >

Parameter: Payment Terms

Update

Parameter Name **Payment Terms** ☒ Audit Enabled

Context Information

Recommended Values

Changes

Previous 1-10 Next 10

| Instance | Organization | | Value | | | Updated On | Updated By |
|----------|----------------|-------------------------------|-------------|-------|--------------------------|----------------------|------------|
| | Type | Name | Recommended | Prior | Current | | |
| Current | Operating Unit | Singapore Distribution Center | | | 45 Net (terms date + 45) | 05-May-1997 16:34:54 | FIN10 |
| Current | Operating Unit | Vision Services R+D | | | 45 Net (terms date + 45) | 15-Dec-1999 12:26:49 | SERVICES |
| Current | Operating Unit | Vision Brazil | | | | 19-Jan-2000 09:14:35 | BRAZIL |
| Current | Operating Unit | Vision Services | | | 45 Net (terms date + 45) | 31-Mar-2000 01:25:15 | SERVICES |

Reporting Groups

A Reporting Group is a user defined group of setup parameters. For example, an IT manager can create a Reporting Group “Purchasing Parameters” for all purchasing related Setup Parameters. Through tracking these Setup Parameters as a group, an IT manager can also analyze and report on changes to the parameters as a group.

To Set up a Reporting Group

| Topic | Navigation Path |
|--------------------------|---|
| Define a Reporting Group | Using the IT Auditor (or equivalent) responsibility, drill into the Setup tab and then the Reporting Groups subtab [Reporting Groups Window]. |

Once the basic attributes of the Reporting Group have been setup (like its Name and dates of validity), click the Add Parameters button to append Setup Parameters to the group.

Application Controls

Setup

Setup Groups | Reporting Groups | Instances

Setup: Reporting Groups > Reporting Group: Order to Cash Reporting Group >

Reporting Group: Payables Group

Update

Reporting Group Name Payables Group

Start Date

Description

End Date

Add Parameter

| Application | Setup Group | Parameter | Updated By | Remove |
|-------------|------------------|----------------------------|---------------------|--------|
| Payables | Payables Options | Exchange Rate Type | Frazier, Mr. Landon | |
| Payables | Payables Options | Pay Group | Frazier, Mr. Landon | |
| Payables | Payables Options | Prepayment Settlement Days | Frazier, Mr. Landon | |
| Payables | Payables Options | Primary Accounting Method | Frazier, Mr. Landon | |
| Payables | Payables Options | Transfer to GL | Frazier, Mr. Landon | |

For example, a "Payables" Reporting Group will typically involve several parameters taken from Payables Setup tables. However, the parameters in a Reporting Group can come from multiple Setup Groups. Note that the same parameter can exist in multiple Reporting Groups.

Remote Application Instances

Application Controls Monitoring can be used to query and report on application control changes in multiple instances. The results can be viewed in a dashboard that compares values of particular Setup Parameters across instances and is therefore particularly useful in troubleshooting configuration problems. The control values can simultaneously be checked against recommended values as well.

Application Controls

Setup

Reporting Group | Application | User | Instance

Compare Application Controls Across Instances

Show Search Criteria

Expand All | Collapse All

| Focus | Setup Group | Current | fin115p2 |
|-------|--|----------|----------|
| | Setup Group | | |
| | AR System Parameters | | |
| | Finance Charge Activity | | |
| | AutoCash Rule Set | | |
| | Vision Operations | Standard | Standard |
| | Days in Days Sales Outstanding Calculation | | |
| | Vision Operations | x 360 | 365 |
| | Address Validation | | |
| | Bank Account Payment Method | | |
| | Vision Operations | x 1363 | ACH |

Before you can view the setup values in remote instances, you need to first import those values to the "current" instance.

Application Controls Monitoring distinguishes between "current" and "remote" instances as follows: the instance that you are presently accessing is the current instance. All other instances that are executing the application with the Setup Parameters of interest are remote in relation to this current instance.

To Import Setup Data from Remote Application Instances

Execute the following two steps to complete the process:

Step 1

Before you can import setup data to the current instance, Application Controls Monitoring requires that you identify the remote instances.

| Topic | Navigation Path |
|---|--|
| Define Remote Instance within Application Controls Monitoring | Using the IT Auditor (or equivalent) responsibility, drill into the Setup tab and then the Instances subtab [Remote Application Instances Window]. Finally, click the Create Instance button. |

The following table provides further information on select fields in the Create Instance window.

| Field | Description |
|---------------|--|
| Instance Code | A unique identifier for distinguishing the instance. It is the Primary key of the ITA_INSTANCES_B table. The Instance Code is generated by default but can be changed to any other unique key. |
| DBC File Name | The DBC (Database Connection) file is a text file which stores all the information required to connect to a particular database. It allows an administrator to easily load groups of environment variable settings. The "Transfer setup attribute from Remote Instances" concurrent program uses this file to connect to the remote instance. The DBC File Name must be unique and the file itself must be stored in the FND_TOP directory. |

All remote instances that are running the application with the Setup Parameters being tracked must be defined. Use the Remote Application Instances window to update or remove the remote instance.

Application Controls **Setup**

Setup Groups | Reporting Groups | **Instances**

Remote Application Instances

Simple Search
Please note that the search is case insensitive.

Instance Name

| Instance ▲ | DBC File Name | Update | Remove |
|------------|-----------------------|--------|--------|
| Unit Test | ap649sdb_fin115p2.dbc | | |

Note that the current instance is not viewable in this window.

Step 2

Periodically, run the concurrent program "Transfer Setup Attributes from Remote Instances." This program imports data from the remote instances defined in Step 1 to the "current" instance.

Note that the transferred data is as current as the last import.

Note on Processing Business Events

The audit trail data transfer from the Shadow Tables to the Change Data Storage Tables is asynchronous. Although the phase of this event subscription is seeded by Oracle at "99" i.e. the highest priority, there is typically a lag between the time events raised on the Shadow Tables are placed on the queue and subsequently picked up by the Agent Listener.

Before analyzing any of the application control changes, you can confirm that the changes have been transferred to Oracle Internal Controls Manager i.e. all raised events are processed. We recommend you periodically perform the following three tasks in Oracle Workflow.

1. Ensure that the subscription to the events raised on Shadow Tables is "Enabled."

| Topic | Navigation Path |
|--|---|
| Checking the status of Event Subscriptions | <p>Using the Workflow Administrator (or equivalent) responsibility, click the Business Events tab and search for the "oracle.apps.ita.setup.record" event [Events Window].</p> <p>Subsequently, drill down into the event by clicking the subscription icon [Update Event Subscription Window].</p> |

[Home](#)
[Developer Studio](#)
[Business Events](#)
[Status Monitor](#)
[Notifications](#)
[Administration](#)

[Events](#)
[Subscriptions](#)
[Agents](#)
[Systems](#)
[Subscriptions](#)
[Subscriptions](#)

[Business Events: Events](#) > [Business Events: Events](#) >

Subscriptions: Event: oracle.apps.ita.setup.record

An event subscription is a registration indicating that a particular event is significant to a particular system. An event subscription specifies the processing to perform when the triggering event occurs.

Create Subscription

| System | Source Type | Out Agent | To Agent | Function | Workflow | Status |
|------------------------|-------------|-----------|----------|----------|----------|---|
| U11510C2.US.ORACLE.COM | Local | | | | | Enabled  |

[Return to Events](#)

- If necessary, change the Status of the Event's subscription to Enabled. Note that to execute this task you must be logged in as a System Administrator or user with Update privileges.
- Ensure that Workflow Agent Listener is "Available."


| Topic | Navigation Path |
|--|--|
| Checking the status of the Workflow Agent Listener | Using the Workflow Administrator Web Applications (or equivalent) responsibility, drill into the Workflow Manager [Applications Dashboard Window]. Note the status of the Agent Listener. |


[Applications Dashboard](#)
[Site Map](#)




[Applications System: fntest](#) >




[Workflow Metrics](#)
[Related Links](#)

Workflow System: fntest


Last Update: 26-01-2005 12:00:05 

Submit Request For: Background Engine 

Notification Mailers  Down
 Agent Listener  Up
 Service Components  Down

Background Engines  Down
 Process  Up
 Control Center Objects  Up

Related Database Parameters

| Parameter Name | Parameter Value | Recommended Value | Description |
|---------------------|-----------------|---|-------------------------------------|
| job_queue_processes | 1 |  | number of job queue slots available |
| job_queue_processes | 5 | | number of AGT jobs Manager to start |

Workflow Metrics

[Work Items](#)
[Show](#)

Agent Activity

[Show](#)

Related Links

[Configuration](#)
[Service Components](#)
[Queue Configuration](#)

Throughput

[Work Items](#)
[Agent Activity](#)
[Notification Mailers](#)

[Return to Top](#)

- If the Agent Listener is "Unavailable" or "Down," click on the Service Components configuration link. In the resulting Service Components window, the component configuration that is crucial to Application Controls Monitoring is the "Workflow Deferred Agent Listener." You can restart the Listener from here.

In order to ensure the accurate tracking and comparison of setup data across instances, the event subscription and agent listener described above must be active in every instance where Oracle Internal Controls Manager is installed.

Note: For detailed information on Events and Subscriptions, refer to the Workflow User Guide.

- Monitor event statuses using the Workflow Administrator responsibility. You can review the start time, process time, and activity summary for each event.

Administer Application Controls Management

This chapter covers the following topics:

- Introduction
- Using Application Controls Monitoring

Introduction

This chapter describes using Application Controls Monitoring to manage critical application controls changes in the Oracle E-Business Suite. Before you can investigate the application controls environment, it is necessary that the setup and implementation of Application Controls Monitoring itself be complete.

Note: For detailed information on implementing Application Controls Monitoring, refer to Setup of Application Controls Management, page 18-1.

Using Application Controls Monitoring

Once the definition of Application Controls Monitoring is complete, you can use the application to query setup changes in your data. Application Controls Monitoring allows you to search for application control values and changes in those values using primarily four criteria:

- Reporting Group
- Application
- User
- Instance

Each of these criteria is a subtab under the main Application Controls tab.

Application Controls Management Query Details

Within the broad criteria mentioned above, you may further narrow down your search results by using the following entities:

- Setup Group
- Setup Parameter

- GL Period
- Instance
- Organizations

As an example, when querying by Reporting Group you can restrict your search results to the Setup Parameters within a particular Setup Group. If any of these entities are left blank, Application Controls Monitoring assumes the default of "All" for that particular criterion.

The screenshot shows the 'Browse Application Controls Changes by Reporting Group' window. The top navigation bar includes 'Reporting Group', 'Applicator', 'User', and 'Instance'. The main title is 'Browse Application Controls Changes by Reporting Group'. Below the title, there are filters for 'Reporting Group' (set to 'Reveles Group'), 'Setup Group' (set to 'Reveles Options'), and 'Parameters' (set to 'All'). There are also fields for 'Period' and 'From' (set to '19-Jun-2020'). A checkbox 'Show only Parameters with current values different from the recommended' is checked. Below the filters, there is a list of Organizations with a search bar and a list of Organizations. The list includes 'Vision Brazil', 'Vision Canada', 'Vision China', 'Vision France', 'Vision Germany', 'Vision India', 'Vision Italy', 'Vision Japan', 'Vision Korea', 'Vision Mexico', 'Vision Netherlands', 'Vision Norway', 'Vision Poland', 'Vision Portugal', 'Vision Project Manufacturing', and 'Vision Sweden'. To the right of the list is a 'Vision Operations' window. Below the list is a table with columns: 'Details', 'Setup Group', 'Parameter', 'Organization', 'Value', 'Last Updated On', and 'Last Updated By'. The table shows a single row with the value 'No search conducted'.

| Details | Setup Group | Parameter | Organization | Value | Last Updated On | Last Updated By |
|----------------------|-------------|-----------|--------------|-------|-----------------|-----------------|
| No search conducted. | | | | | | |

Note that the LOV for the GL period show all periods irrespective of the period set. However, you can restrict the results to a particular period set in the GL period LOV window.

Viewing Query Results

Application Controls Monitoring enables you to administer Application Controls (setups) by viewing particular control values in relation to their prior and benchmarked values.

In the dashboard view, if the current value of a particular Setup Parameter does not equal its recommended value, Oracle Internal Controls Manager displays a red cross next to that value. With the aid of this flag, a quick scan of the dashboard can alert a user to the Setup Parameter that must be investigated.

| Application Controls Setup | | | | | | | | | |
|--|---------------------------|----------------|-------------------|--------------|-------------|-------|-------------------|---------------------|-----------------|
| Reporting Group Application User Instance | | | | | | | | | |
| Browse Application Controls Changes by Reporting Group | | | | | | | | | |
| Show Search Criteria | | | | | | | | | |
| Details | Setup Group | Parameter | Type | Organization | Recommended | Prior | Value | Last Updated On | Last Updated By |
| Show Payables Options | Primary Accounting Method | Operating Unit | Vision Operations | | | | Accrual | 1-Jul-2008 12:20:08 | |
| Show Payables Options | Primary Accounting Method | Operating Unit | Vision Operations | | | | | 17-Jan-2008 AUDITOR | 16:28:20 |
| Show Payables Options | Exchange Rate Type | Operating Unit | Vision Operations | Cust | | | Corporate User | 10-Jan-2008 AUDITOR | 15:54:56 |
| Show Payables Options | Transfer to GL | Operating Unit | Vision Operations | In Detail | | | In Detail | 18-Jan-2008 AUDITOR | 15:55:37 |
| Show Payables Options | Pay Group | Operating Unit | Vision Operations | EMF_LG_01 | | | DOV=ST C=EMPL01EE | 10-Jan-2008 AUDITOR | 14:11:32 |

You can then make corrections and/or adjustments to the application control data i.e. the setups accordingly.

Note: The changes to the application control data settings must be performed within the appropriate Oracle E-Business Suite module.

Querying Application Controls in Multiple Instances

Application Controls Monitoring queries are typically run within a specific instance. However, you can use the menu path Application Controls > Instances to query and view the values of Setup Parameters in upto four instances simultaneously.

| Application Controls Setup | | | | | | | | | |
|---|--|---------|--|------------|--|--|--|--|--|
| Reporting Group Application User Instance | | | | | | | | | |
| Compare Application Controls Across Instances | | | | | | | | | |
| Show Search Criteria | | | | | | | | | |
| Expand All Collapse All | | | | | | | | | |
| | | | | | | | | | |
| Focus | Setup Group | Current | | fin115p2 | | | | | |
| | Setup Group | | | | | | | | |
| | AR System Parameters | | | | | | | | |
| | Finance Charge Activity | | | | | | | | |
| | AutoCash Rule Set | | | | | | | | |
| | Vision Operations | | | Standard | | | | | |
| | Days in Days Sales Outstanding Calculation | | | | | | | | |
| | Vision Operations | | | X 360 365 | | | | | |
| | Address Validation | | | | | | | | |
| | Bank Account Payment Method | | | | | | | | |
| | Vision Operations | | | X 1363 ACH | | | | | |

Again, a quick scan of the dashboard can alert a user to the Setup Parameter and Instance that must be investigated.

Application Controls Monitoring Implementation Checklist

This chapter covers the following topics:

- Introduction
- Checklist Steps

Introduction

This chapter contains a checklist of tasks that must be executed to complete the implementation of Application Controls Monitoring.

When you install Oracle Internal Controls Manager, the installation process automatically creates the responsibility "IT Auditor." This responsibility includes the necessary functions to setup and implement the application. Hence as a prerequisite step, setup the appropriate users by assigning them this responsibility for the implementation.

Note: Concurrent programs are generally administered by the Oracle Applications System Administrator.

Since some implementation steps build upon information you define in prior implementation steps, you should perform the steps in the order listed.

Checklist Steps

The following table lists the steps required to implement Application Controls Monitoring.

Note: For detailed information on each of these steps, refer to Setup of Application Controls Management, page 18-1.

| Description | Required | Optional |
|--|----------|----------|
| Prerequisite Steps | | |
| Step 1 - Run the concurrent program AuditTrail Update Tables | X | |
| Step 2 - Set the profile option Audit Trail: Activate to "Yes" at the Site level | X | |
| Step 3 - Run the concurrent program ITA Enable Setup Change Tracking | X | |
| Setup Groups and Parameters | | |
| Step 4 - Review seeded Setup Groups for Application Controls Monitoring | | X |
| Step 5 - Review seeded Setup Parameters for Application Controls Monitoring | | X |
| Step 6 - Enter recommended values for Setup Parameters | | X |
| Reporting Groups | | |
| Step 7 - Define Reporting Groups | | X |
| Remote Application Instances | | |
| Step 8 - Define Remote Application Instances | | X |
| Step 9 - Run the concurrent program Transfer Setup Attributes from Remote Instances. | | X |

Seeded Setup Groups and Parameters

This chapter covers the following topics:

- Introduction
- Setup Group Detail Listings

Introduction

The Application Controls Management feature enables IT managers and auditors to track changes to Setup Parameters in several modules within the Oracle E-Business Suite.

The following sections provide a detailed listing of the specific Setup Groups, Applications, and Setup Parameters that can be audited for changes.

Note: Only the most significant parameters in each group are shown.

Setup Group Detail Listings

Setup Group Name: Financials Options

Application: AP

Table Name: FINANCIALS_SYSTEM_PARAMS_ALL

| Setup Parameter Name | Column Name |
|-----------------------------|------------------------------|
| Always Take Discount | ALWAYS_TAKE_DISC_FLAG |
| Pay Alone | EXCLUSIVE_PAYMENT_FLAG |
| RFQ Only Site | RFQ_ONLY_SITE_FLAG |
| Hold Unmatched Invoices | HOLD_UNMATCHED_INVOICES_FLAG |
| Invoice Match Option | MATCH_OPTION |
| Supplier Number Creation | USER_DEFINED_VENDOR_NUM_CODE |
| Supplier Number Type | MANUAL_VENDOR_NUM_TYPE |
| Use Requisition Encumbrance | REQ_ENCUMBRANCE_FLAG |
| Reserve at Completion | RESERVE_AT_COMPLETION_FLAG |
| Use PO Encumbrance | PURCH_ENCUMBRANCE_FLAG |

| Setup Parameter Name | Column Name |
|-------------------------------|--------------------------------|
| Payment Terms | TERMS_ID |
| Payment Method | PAYMENT_METHOD_LOOKUP_CODE |
| Ship-To Location | SHIP_TO_LOCATION_ID |
| Bill-To Location | BILL_TO_LOCATION_ID |
| Ship Via | SHIP_VIA_LOOKUP_CODE |
| FOB | FOB_LOOKUP_CODE |
| Liability Account | ACCTS_PAY_CODE_COMBINATION_ID |
| Prepayment Account | PREPAY_CODE_COMBINATION_ID |
| Discount Taken Account | DISC_TAKEN_CODE_COMBINATION_ID |
| Future Periods | FUTURE_PERIOD_LIMIT |
| Requisition Encumbrance Type | REQ_ENCUMBRANCE_TYPE_ID |
| PO Encumbrance Type | PURCH_ENCUMBRANCE_TYPE_ID |
| Invoice Encumbrance Type | INV_ENCUMBRANCE_TYPE_ID |
| Inventory Organization | INVENTORY_ORGANIZATION_ID |
| Freight Terms | FREIGHT_TERMS_LOOKUP_CODE |
| Receipt Acceptance Days | RECEIPT_ACCEPTANCE_DAYS |
| Business Group | BUSINESS_GROUP_ID |
| Expense Reimbursement Address | EXPENSE_CHECK_ADDRESS_FLAG |
| Use Approval Hierarchies | USE_POSITIONS_FLAG |
| VAT Registration Number | VAT_REGISTRATION_NUM |
| VAT Registration Member State | VAT_COUNTRY_CODE |
| PO Rate Variance Gain Account | RATE_VAR_GAIN_CCID |
| PO Rate Variance Loss Account | RATE_VAR_LOSS_CCID |
| Default Tax Code | VAT_CODE |
| Enable Recoverable Tax | NON_RECOVERABLE_TAX_FLAG |
| Tax Rounding Rule | TAX_ROUNDING_RULE |
| Precision | PRECISION |
| Min Accountable Unit | MINIMUM_ACCOUNTABLE_UNIT |
| Default Recovery Rate | DEFAULT_RECOVERY_RATE |
| Future Dated Payment Account | FUTURE_DATED_PAYMENT_CCID |

| Setup Parameter Name | Column Name |
|--------------------------|-----------------------|
| Expense Clearing Account | EXPENSE_CLEARING_CCID |
| Miscellaneous Account | MISC_CHARGE_CCID |

Setup Group Name: Payables Options

Application: AP

Table Name: AP_SYSTEM_PARAMETERS_ALL

| Setup Parameter Name | Column Name |
|--|--------------------------------|
| Primary Accounting Method | ACCOUNTING_METHOD_OPTION |
| Secondary Accounting Method | SECONDARY_ACCOUNTING_METHOD |
| Automatic Offset Method | LIABILITY_POST_LOOKUP_CODE |
| Prevent Prepayment Application Across Balancing Segments | STOP_PREPAY_ACROSS_BAL_FLAG |
| Set of Books | SET_OF_BOOKS_ID |
| Transfer to GL | GL_TRANSFER_MODE |
| Transfer Reporting Books | INCLUDE_REPORTING_SOB |
| Submit Journal Import | GL_TRANSFER_SUBMIT_JOURNAL_IMP |
| Allow Override at Program Submission | GL_TRANSFER_ALLOW_OVERRIDE |
| Account for Payment - When Payment is Issued | WHEN_TO_ACCOUNT_PMT |
| Account for Payment - When Payment Clears | RECON_ACCOUNTING_FLAG |
| Account for Gain/Loss - When Payment is Issued | WHEN_TO_ACCOUNT_GAIN_LOSS |
| Account for Gain/Loss - When Payment Clears | RECON_ACCOUNTING_FLAG |
| Gain/Loss Calculation | GAIN_LOSS_CALC_LEVEL |
| Use Future Dated Payment Account | FUTURE_DATED_PMT_ACCT_SOURCE |
| Use Multiple Currencies | MULTI_CURRENCY_FLAG |
| Require Exchange Rate Entry | MAKE_RATE_MANDATORY_FLAG |
| Calculate User Exchange Rate | CALC_USER_XRATE |
| Exchange Rate Type | DEFAULT_EXCHANGE_RATE_TYPE |
| Realized Gain Account | GAIN_CODE_COMBINATION_ID |
| Realized Loss Account | LOSS_CODE_COMBINATION_ID |
| Rounding Account | ROUNDING_ERROR_CCID |
| Pay Group | VENDOR_PAY_GROUP_LOOKUP_CODE |
| Invoice Currency | INVOICE_CURRENCY_CODE |

| Setup Parameter Name | Column Name |
|---|--------------------------------|
| Terms Date Basis | TERMS_DATE_BASIS |
| Pay Date Basis | PAY_DATE_BASIS_LOOKUP_CODE |
| Bank Charge Bearer | BANK_CHARGE_BEARER |
| Combined Filing Program | COMBINED_FILING_FLAG |
| Use Pay Site Tax Region | INCOME_TAX_REGION_FLAG |
| Income Tax Region | INCOME_TAX_REGION |
| Use Invoice Approval Workflow | APPROVAL_WORKFLOW_FLAG |
| Allow Force Approval | ALLOW_FORCE_APPROVAL_FLAG |
| Require Validation Before Approval | VALIDATE_BEFORE_APPROVAL_FLAG |
| Allow Adjustments to Paid Invoices | ALLOW_PAID_INVOICE_ADJUST |
| Recalculate Scheduled Payment | RECALC_PAY_SCHEDULE_FLAG |
| Automatically Create Freight Distribution | AUTO_CREATE_FREIGHT_FLAG |
| GL Date Basis | GL_DATE_FROM_RECEIPT_FLAG |
| Confirm Date as Invoice Number | CONFIRM_DATE_AS_INV_NUM_FLAG |
| Allow Online Validation | APPROVALS_OPTION |
| Allow Document Category Override | INV_DOC_CATEGORY_OVERRIDE |
| Prepayment Payment Terms | PREPAYMENT_TERMS_ID |
| Prepayment Settlement Days | ADD_DAYS_SETTLEMENT_DATE |
| Build Prepayment Accounts when Matching | BUILD_PREPAYMENT_ACCOUNTS_FLAG |
| Freight Account | FREIGHT_CODE_COMBINATION_ID |
| Allow Final Matching | ALLOW_FINAL_MATCH_FLAG |
| Allow Distribution Level Matching | ALLOW_DIST_MATCH_FLAG |
| Allow Matching Account Override | ALLOW_FLEX_OVERRIDE_FLAG |
| Transfer PO Descriptive Flexfield Information | TRANSFER_DESC_FLEX_FLAG |
| Allow Interest Invoices | AUTO_CALCULATE_INTEREST_FLAG |
| Prorate Across Overdue Invoices | PRORATE_INT_INV_ACROSS_DIST |
| Minimum Interest Amount | INTEREST_TOLERANCE_AMOUNT |
| Interest Expense Account | INTEREST_CODE_COMBINATION_ID |
| Interest Liability Account | INTEREST_ACCTS_PAY_CCID |
| Expense Report Default Template | EXPENSE_REPORT_ID |
| Expense Report Payment Terms | EMPLOYEE_TERMS_ID |

| Setup Parameter Name | Column Name |
|--|--------------------------------|
| Expense Report Pay Group | EMPLOYEE_PAY_GROUP_LOOKUP_CODE |
| Employee Payment Priority | EMPLOYEE_PAYMENT_PRIORITY |
| Apply Advances | APPLY_ADVANCES_DEFAULT |
| Automatically Create Employee as Supplier | CREATE_EMPLOYEE_VENDOR_FLAG |
| Hold Unmatched Expense Reports | HOLD_UNMATCHED_INVOICES_FLAG |
| Bank Account | BANK_ACCOUNT_ID |
| Payment Batch Limit | MAX_OUTLAY |
| EFT User Number | EFT_USER_NUMBER |
| Additional Pay Through Days | DAYS_BETWEEN_CHECK_CYCLES |
| Allow Document Category Override | PAY_DOC_CATEGORY_OVERRIDE |
| Exclude Tax From Discount | DISC_IS_INV_LESS_TAX_FLAG |
| Discount Method | DISCOUNT_DISTRIBUTION_METHOD |
| Allow Print | ONLINE_PRINT_FLAG |
| Allow Pre-Date | POST_DATED_PAYMENTS_FLAG |
| Allow Address Change | UPDATE_PAY_SITE_FLAG |
| Allow Void and Reissue | REPLACE_CHECK_FLAG |
| XML Payments - Automatic Configuration | XML_PAYMENTS_AUTO_CONFIRM_FLAG |
| Allow Remit to Account Override | ALLOW_SUPPLIER_BANK_OVERRIDE |
| Use Bank Charges | USE_BANK_CHARGE_FLAG |
| Require Tax Entry at Header | REQUIRE_TAX_ENTRY_FLAG |
| Allow Calculation Override | AUTO_TAX_CALC_OVERRIDE |
| Allow Override | AMOUNT_INCLUDES_TAX_OVERRIDE |
| Distribution Amounts Include Tax | AMOUNT_INCLUDES_TAX_FLAG |
| Use Withholding Tax | ALLOW_AWT_FLAG |
| Allow Manual Withholding | ALLOW_AWT_OVERRIDE |
| Include Discount Amount | AWT_INCLUDE_DISCOUNT_AMT |
| Include Tax Amount | AWT_INCLUDE_TAX_AMT |
| Tax Group | DEFAULT_AWT_GROUP_ID |
| Apply Withholding Tax | CREATE_AWT_DISTS_TYPE |
| Create Withholding Invoice | CREATE_AWT_INVOICES_TYPE |
| Include Income Tax Type on Withholding Distributions | ENABLE_1099_ON_AWT_FLAG |

| Setup Parameter Name | Column Name |
|---|------------------------------|
| Enforce Tax From Account | ENFORCE_TAX_FROM_ACCOUNT |
| Enforce Tax From Purchase Order | MATCH_ON_TAX_FLAG |
| Tax Code Defaults - PO for Matched Invoices | TAX_FROM_PO_FLAG |
| Tax Code Defaults - PO for Matched Invoices Hierarchy | TAX_HIER_PO_SHIPMENT |
| Tax Code Defaults - Supplier Site | TAX_FROM_VENDOR_SITE_FLAG |
| Tax Code Defaults - Supplier Site Hierarchy | TAX_HIER_VENDOR_SITE |
| Tax Code Defaults - Supplier | TAX_FROM_VENDOR_FLAG |
| Tax Code Defaults - Supplier Hierarchy | TAX_HIER_VENDOR |
| Tax Code Defaults - Account | TAX_FROM_ACCOUNT_FLAG |
| Tax Code Defaults - Account Hierarchy | TAX_HIER_ACCOUNT |
| Tax Code Defaults - Financials | TAX_FROM_SYSTEM_FLAG |
| Tax Code Defaults - Financials Hierarchy | TAX_HIER_SYSTEM |
| Tax Code Defaults - Invoice Header | TAX_FROM_INV_HEADER_FLAG |
| Tax Code Defaults - Invoice Header Hierarchy | TAX_HIER_INVOICE |
| Tax Code Defaults - Template | TAX_FROM_TEMPLATE_FLAG |
| Tax Code Defaults - Template Hierarchy | TAX_HIER_TEMPLATE |
| Relieve Future Dated Payment Liability | FUTURE_DATED_PMT_LIAB_RELIEF |
| Sort By Alternate Field | SORT_BY_ALTERNATE_FIELD |

Setup Group: Receivables Options

Application: AR

Table Name: AR_SYSTEM_PARAMETERS_ALL

| Setup Parameter Name | Column Name |
|-----------------------------|----------------------------|
| Accounting Method | ACCOUNTING_METHOD |
| Automatic Journal Import | RUN_GL_JOURNAL_IMPORT_FLAG |
| Days per Posting Cycle | POSTING_DAYS_PER_CYCLE |
| Finance Charge Activity | FINCHRG_RECEIVABLES_TRX_ID |
| Realized Gains Account | CODE_COMBINATION_ID_GAIN |
| Realized Losses Account | CODE_COMBINATION_ID_LOSS |
| Tax Account | LOCATION_TAX_ACCOUNT |
| Unallocated Revenue Account | UNALLOCATED_REVENUE_CCID |

| Setup Parameter Name | Column Name |
|--|-------------------------------|
| Cross Currency Rate Type | CROSS_CURRENCY_RATE_TYPE |
| Cross Currency Rounding Account | CODE_COMBINATION_ID_ROUND |
| Header Rounding Account | TRX_HEADER_ROUND_CCID |
| Header Level Rounding | TRX_HEADER_LEVEL_ROUNDING |
| Tax Method | TAX_METHOD |
| From Postal Code | FROM_POSTAL_CODE |
| To Postal Code | TO_POSTAL_CODE |
| Address Validation | ADDRESS_VALIDATION |
| Compound Taxes | TAX_INVOICE_PRINT |
| Tax Registration Number | TAX_REGISTRATION_NUMBER |
| Tax Vendor Views | TAX_DATABASE_VIEW_SET |
| Sales Tax Geo Override | SALES_TAX_GEOCODE |
| Inclusive Tax Used | INCLUSIVE_TAX_USED |
| Tax Calculation Level | TAX_HEADER_LEVEL_FLAG |
| Tax Rounding Rule | TAX_ROUNDING_RULE |
| Tax Reporting Currency | TAX_CURRENCY_CODE |
| Tax Precision | TAX_PRECISION |
| Tax Min Accountable Unit | TAX_MINIMUM_ACCOUNTABLE_UNIT |
| Allow Override | TAX_ROUNDING_ALLOW_OVERRIDE |
| Enforce Tax from Revenue Account | TAX_ENFORCE_ACCOUNT_FLAG |
| Calculate Tax on Credit &Memo during Autoinvoice | CALC_TAX_ON_CREDIT_MEMO_FLAG |
| Tax Code Defaults - Customer Site | TAX_USE_SITE_EXC_RATE_FLAG |
| Tax Code Defaults - Customer Site Hierarchy | TAX_HIER_SITE_EXC_RATE |
| Tax Code Defaults - Customer | TAX_USE_CUST_EXC_RATE_FLAG |
| Tax Code Defaults - Customer Hierarchy | TAX_HIER_CUST_EXC_RATE |
| Tax Code Defaults - Product | TAX_USE_PROD_EXC_RATE_FLAG |
| Tax Code Defaults - Product Hierarchy | TAX_HIER_PROD_EXC_RATE |
| Tax Code Defaults - Revenue Account | TAX_USE_ACCOUNT_EXC_RATE_FLAG |
| Tax Code Defaults - Revenue Account Hierarchy | TAX_HIER_ACCOUNT_EXC_RATE |
| Tax Code Defaults - System Options | TAX_USE_SYSTEM_EXC_RATE_FLAG |

| Setup Parameter Name | Column Name |
|---|--------------------------------|
| Tax Code Defaults - System Options Hierarchy | TAX_HIER_SYSTEM_EXC_RATE |
| Tax Code | TAX_CODE |
| Use Customer Exemptions | TAX_USE_CUSTOMER_EXEMPT_FLAG |
| Use Item Exemptions | TAX_USE_PRODUCT_EXEMPT_FLAG |
| Use Item Rate Exemptions | TAX_USE_LOC_EXC_RATE_FLAG |
| Allow Changes to Printed Transactions | CHANGE_PRINTED_INVOICE_FLAG |
| Allow Payment of Unrelated Transaction | PAY_UNRELATED_INVOICES_FLAG |
| Allow Transaction Deletion | INVOICE_DELETION_FLAG |
| Show Billing Number | SHOW_BILLING_NUMBER_FLAG |
| Document Number Generation Level | DOCUMENT_SEQ_GEN_LEVEL |
| AutoInvoice Accounting Flex Segment | AI_ACCT_FLEX_KEY_LEFT_PROMPT |
| AutoInvoice System Items Flex Segment | AI_MTL_ITEMS_KEY_LEFT_PROMPT |
| AutoInvoice Territory Flex Segment | AI_TERRITORY_KEY_LEFT_PROMPT |
| AutoInvoice Max Memory in Bytes | AI_MAX_MEMORY_IN_BYTES |
| AutoInvoice Purge Interface Tables | AI_PURGE_INTERFACE_TABLES_FLAG |
| Log File Message Level | AI_LOG_FILE_MESSAGE_LEVEL |
| Automatic Customer Numbering | GENERATE_CUSTOMER_NUMBER |
| Automatic Customer Site Numbering | AUTO_SITE_NUMBERING |
| Create Reciprocal Customer | CREATE_RECIPROCAL_FLAG |
| Customer Grouping Rule | DEFAULT_GROUPING_RULE_ID |
| Standard Refund Policy Days | STANDARD_REFUND |
| Payment Term Threshold Days | PAYMENT_THRESHOLD |
| Credit Classification for Deferring Revenue - First Selection | CREDIT_CLASSIFICATION1 |
| Credit Classification for Deferring Revenue - Second Selection | CREDIT_CLASSIFICATION2 |
| Credit Classification for Deferring Revenue - Third Selection | CREDIT_CLASSIFICATION3 |
| Prepare for Claim Creation | UNMTCH_CLAIM_CREATION_FLAG |
| Match Remittance Lines | MATCHED_CLAIM_CREATION_FLAG |
| Exclude Credit Memos | MATCHED_CLAIM_EXCL_CM_FLAG |
| Split Amount | CER_SPLIT_AMOUNT |
| Discount Basis | CALC_DISCOUNT_ON_LINES_FLAG |

| Setup Parameter Name | Column Name |
|--|-------------------------------|
| AutoCash Rule Set | AUTOCASH_HIERARCHY_ID |
| Days in Days Sales Outstanding Calculation | CER_DSO_DAYS |
| Sales Credit Percent Limit | SALES_CREDIT_PCT_LIMIT |
| Min Write off Limits per Receipt | MIN_WRTOFF_AMOUNT |
| Max Write off Limits per Receipt | MAX_WRTOFF_AMOUNT |
| Accrue Interest | ACCRUE_INTEREST |
| Allow Unearned Discounts | UNEARNED_DISCOUNT |
| Discount On Partial Payment | PARTIAL_DISCOUNT_FLAG |
| Trade Accounting Installed | TA_INSTALLED_FLAG |
| Bills Receivable Enabled | BILLS_RECEIVABLE_ENABLED_FLAG |
| Require Salesperson | SALESREP_REQUIRED_FLAG |
| Require Billing Location for Receipts | SITE_REQUIRED_FLAG |
| Print Remit to Address | PRINT_REMIT_TO |
| Print Home Country | PRINT_HOME_COUNTRY_FLAG |
| Minimum Refund Amount | MIN_REFUND_AMOUNT |
| Credit Card Payment Method | IREC_CC_RECEIPT_METHOD_ID |
| Bank Account Payment Method | IREC_BA_RECEIPT_METHOD_ID |
| Invoices Per Commit | AUTO_REC_INVOICES_PER_COMMIT |
| Receipts Per Commit | AUTO_REC_RECEIPTS_PER_COMMIT |
| Chargeback Due Date | DEFAULT_CB_DUE_DATE |
| Default Country | DEFAULT_COUNTRY |
| Source of Territory | DEFAULT_TERRITORY |
| Application Rule Set | RULE_SET_ID |

Setup Group Name: Cash Parameters

Application: CE

Table Name: CE_SYSTEM_PARAMETERS_ALL

| Setup Parameter Name | Column Name |
|-----------------------------------|------------------------------|
| Set Of Books | SET_OF_BOOKS_ID |
| Begin Date | CASHBOOK_BEGIN_DATE |
| Show Cleared Transactions | SHOW_CLEARED_FLAG |
| Tolerance Amount | AMOUNT_TOLERANCE |
| Tolerance Percent | PERCENT_TOLERANCE |
| Receivable Activity | RECEIVABLES_TRX_ID |
| AP Tolerance Difference | DIFFERENCES_ACCOUNT |
| Lines Per Commit | LINES_PER_COMMIT |
| Purge Interface | INTERFACE_PURGE_FLAG |
| Archive Interface | INTERFACE_ARCHIVE_FLAG |
| Add Lines to Automatic Statements | LINE_AUTOCREATION_FLAG |
| Use Reconciliation Open Interface | ENABLE_OPEN_INTERFACE_FLAG |
| Foreign Tolerance Difference | FOREIGN_DIFFERENCE_HANDLING |
| Payables Matching Order | AP_MATCHING_ORDER |
| Receivables Matching Order | AR_MATCHING_ORDER |
| Open Interface Float Status | OPEN_INTERFACE_FLOAT_STATUS |
| Open Interface Clear Status | OPEN_INTERFACE_CLEAR_STATUS |
| Float Handling | FLOAT_HANDLING_FLAG |
| Show Void Payments | SHOW_VOID_PAYMENT_FLAG |
| Open Interface Matching Criteria | OPEN_INTERFACE_MATCHING_CODE |
| Exchange Rate Type | EXCHANGE_RATE_TYPE |
| Exchange Rate Date | EXCHANGE_RATE_DATE |

Setup Group Name: Set of Books

Application: GL

Table Name: GL_Sets_Of_Books

| Setup Parameter Name | Column Name |
|---|--------------------------------|
| Functional Currency | CURRENCY_CODE |
| Chart of Accounts | CHART_OF_ACCOUNTS_ID |
| Name | NAME |
| Calendar Name | PERIOD_SET_NAME |
| Suspense | SUSPENSE_ALLOWED_FLAG |
| Short Name | SHORT_NAME |
| Require Budget Journals | REQUIRE_BUDGET_JOURNALS_FLAG |
| Enable Budgetary Control | ENABLE_BUDGETARY_CONTROL_FLAG |
| Balance Intercompany Journals | ALLOW_INTERCOMPANY_POST_FLAG |
| Translation Adjustment | CUM_TRANS_CODE_COMBINATION_ID |
| Future Periods | FUTURE_ENTERABLE_PERIODS_LIMIT |
| Retained Earnings | RET_EARN_CODE_COMBINATION_ID |
| Reserve for Encumbrance | RES_ENCUMB_CODE_COMBINATION_ID |
| Description | DESCRIPTION |
| Enable Average Balances | ENABLE_AVERAGE_BALANCES_FLAG |
| Consolidation Set Of Books | CONSOLIDATION_SOB_FLAG |
| Maintain EOD | TRANSLATE_EOD_FLAG |
| Maintain QATD | TRANSLATE_QATD_FLAG |
| Maintain YATD | TRANSLATE_YATD_FLAG |
| Translation Rate Type | DAILY_TRANSLATION_RATE_TYPE |
| Net Income | NET_INCOME_CODE_COMBINATION_ID |
| Journal Entry Tax | ENABLE_AUTOMATIC_TAX_FLAG |
| Journal Approval | ENABLE_JE_APPROVAL_FLAG |
| Set of Books Type | MRC_SOB_TYPE_CODE |
| Rounding Difference | TRACK_ROUNDING_IMBALANCE_FLAG |
| Rounding Account | ROUNDING_CODE_COMBINATION_ID |
| Secondary Segment Closing and Translation | ENABLE_SECONDARY_TRACK_FLAG |
| Secondary Segment Revaluation | ENABLE_REVAL_SS_TRACK_FLAG |

Setup Group Name: Tax Options

Application: GL

Table Name: GL_Tax_Options

| Setup Parameter Name | Column Name |
|------------------------------|------------------------------|
| Tax Reporting Currency | TAX_CURRENCY_CODE |
| Tax Precision | TAX_PRECISION |
| Minimum Accountable Unit | TAX_MAU |
| Calculation Level | CALCULATION_LEVEL_CODE |
| Allow Rounding Rule Override | ALLOW_ROUNDING_OVERRIDE_FLAG |
| Input Rounding Rule | INPUT_ROUNDING_RULE_CODE |
| Output Rounding Rule | OUTPUT_ROUNDING_RULE_CODE |
| Input Tax Code | INPUT_TAX_CODE |
| Input Amount Includes Tax | INPUT_AMT_INCL_TAX_FLAG |
| Output Tax Code | OUTPUT_TAX_CODE |
| Output Amount Includes Tax | OUTPUT_AMT_INCL_TAX_FLAG |

Setup Group Name: Inventory Parameters

Application: INV

Table Name: Mtl_Parameters

| Setup Parameter Name | Column Name |
|------------------------------|-----------------------------|
| Organization Code | ORGANIZATION_CODE |
| Item Master Organization | MASTER_ORGANIZATION_ID |
| Costing Method | PRIMARY_COST_METHOD |
| Costing Organization | COST_ORGANIZATION_ID |
| Default Material Sub-Element | DEFAULT_MATERIAL_COST_ID |
| Calendar | CALENDAR_CODE |
| Transfer to GL | GENERAL_LEDGER_UPDATE_CODE |
| Default ATP Rule | DEFAULT_ATP_RULE_ID |
| Default Picking Rule | DEFAULT_PICKING_RULE_ID |
| Default Locator Order | DEFAULT_LOCATOR_ORDER_VALUE |
| Default Subinventory Order | DEFAULT_SUBINV_ORDER_VALUE |
| Allow Negative Balances | NEGATIVE_INV_RECEIPT_CODE |
| Locator Control | STOCK_LOCATOR_CONTROL_CODE |
| Material Account | MATERIAL_ACCOUNT |
| Material Overhead Account | MATERIAL_OVERHEAD_ACCOUNT |
| Resource Account | RESOURCE_ACCOUNT |

| Setup Parameter Name | Column Name |
|--|--------------------------------|
| Purchase Price Variance Account | PURCHASE_PRICE_VAR_ACCOUNT |
| Inventory AP Accrual Account | AP_ACCRUAL_ACCOUNT |
| Overhead Account | OVERHEAD_ACCOUNT |
| Outside Processing Account | OUTSIDE_PROCESSING_ACCOUNT |
| Inter-organization Intransit Inventory Account | INTRANSIT_INV_ACCOUNT |
| Inter-organization Receivable Account | INTERORG_RECEIVABLES_ACCOUNT |
| Inter-organization Purchase Price Variance Account | INTERORG_PRICE_VAR_ACCOUNT |
| Inter-organization Payable Account | INTERORG_PAYABLES_ACCOUNT |
| Cost of Goods Sold Account | COST_OF_SALES_ACCOUNT |
| Encumbrance Account | ENCUMBRANCE_ACCOUNT |
| Inter-organization Transfer Credit Account | INTERORG_TRANSFER_CR_ACCOUNT |
| Inter-organization transfer charge | MATL_INTERORG_TRANSFER_CODE |
| Inter-organization transfer percent | INTERORG_TRNSFR_CHARGE_PERCENT |
| Item Sourcing Organization | SOURCE_ORGANIZATION_ID |
| Item Sourcing Subinventory | SOURCE_SUBINVENTORY |
| Item Sourcing Type | SOURCE_TYPE |
| Serial Number Uniqueness | SERIAL_NUMBER_TYPE |
| Serial Number Prefix | AUTO_SERIAL_ALPHA_PREFIX |
| Starting Serial Number | START_AUTO_SERIAL_NUMBER |
| Lot Prefix | AUTO_LOT_ALPHA_PREFIX |
| Lot Number Uniqueness | LOT_NUMBER_UNIQUENESS |
| Lot Number Generation | LOT_NUMBER_GENERATION |
| Lot Number Zero Pad Suffix | LOT_NUMBER_ZERO_PADDING |
| Lot Number Total Length | LOT_NUMBER_LENGTH |
| Starting Revision | STARTING_REVISION |
| Demand Class | DEFAULT_DEMAND_CLASS |
| Reverse Encumbrance | ENCUMBRANCE_REVERSAL_FLAG |
| Invoice Price Variance Account | INVOICE_PRICE_VAR_ACCOUNT |
| Cost Variance Account | AVERAGE_COST_VAR_ACCOUNT |
| Sales Account | SALES_ACCOUNT |
| Expense Account | EXPENSE_ACCOUNT |

| Setup Parameter Name | Column Name |
|--|-------------------------------|
| Serial Number Generation | SERIAL_NUMBER_GENERATION |
| Project Cost Collect. Enabled | PM_COST_COLLECTION_ENABLED |
| Rates Cost Type | AVG_RATES_COST_TYPE_ID |
| Project Clearance Account | PROJECT_COST_ACCOUNT |
| Capacity Load Weight | ORG_MAX_WEIGHT |
| Capacity Volume | ORG_MAX_VOLUME |
| Move Order Timeout Period | TXN_APPROVAL_TIMEOUT_PERIOD |
| Pick Confirmation Required | MO_PICK_CONFIRM_REQUIRED |
| Move Order Timeout Action | MO_APPROVAL_TIMEOUT_ACTION |
| Borrow Payback Material Variance Account | BORRPAY_MATL_VAR_ACCOUNT |
| Borrow Payback Material Overhead Variance Account | BORRPAY_MOH_VAR_ACCOUNT |
| Borrow Payback Resource Variance Account | BORRPAY_RES_VAR_ACCOUNT |
| Borrow Payback Outside Processing Variance Account | BORRPAY_OSP_VAR_ACCOUNT |
| Borrow Payback Overhead Variance Account | BORRPAY_OVH_VAR_ACCOUNT |
| Process Enabled | PROCESS_ENABLED_FLAG |
| Process Organization | PROCESS_ORGN_CODE |
| Default Cost Group | DEFAULT_COST_GROUP_ID |
| WMS Enabled | WMS_ENABLED_FLAG |
| Allocate Serial Numbers | ALLOCATE_SERIAL_FLAG |
| EAM Enabled | EAM_ENABLED_FLAG |
| EAM Organization | MAINT_ORGANIZATION_ID |
| Quality Skipping Inspection Control | QA_SKIPPING_INSP_FLAG |
| Material Overhead Sub-Element | DEFAULT_MATL_OVHD_COST_ID |
| Distributed Organization | DISTRIBUTED_ORGANIZATION_FLAG |
| Carrier Manifesting Organization | CARRIER_MANIFESTING_FLAG |

Setup Group Name: Purchasing Options

Application: PO

Table Name: PO_System_Parameters_All

| Setup Parameter Name | Column Name |
|------------------------------------|--------------------------------|
| Expense AP Accrual Account | ACCRUED_CODE_COMBINATION_ID |
| Price Tolerance Percentage | PRICE_CHANGE_ALLOWANCE |
| REQ_CAN_AUTHORIZE | REQ_CAN_AUTHORIZE |
| INSPECTION_REQUIRED_FLAG | INSPECTION_REQUIRED_FLAG |
| Enforce Price Tolerance Percentage | ENFORCE_PRICE_CHANGE_ALLOWANCE |
| Rate Type | DEFAULT_RATE_TYPE |
| TAXABLE_FLAG | TAXABLE_FLAG |
| Quotation Number Entry | USER_DEFINED_QUOTE_NUM_CODE |
| Quotation Number Type | MANUAL_QUOTE_NUM_TYPE |
| RFQ Number Entry | USER_DEFINED_RFQ_NUM_CODE |
| RFQ Number Type | MANUAL_RFQ_NUM_TYPE |
| PO Number Entry | USER_DEFINED_PO_NUM_CODE |
| PO Number Type | MANUAL_PO_NUM_TYPE |
| Requisition Number Entry | USER_DEFINED_REQ_NUM_CODE |
| Requisition Number Type | MANUAL_REQ_NUM_TYPE |
| Quote Warning Delay | DEFAULT_QUOTE_WARNING_DELAY |
| Enforce Buyer Name | ENFORCE_BUYER_NAME_FLAG |
| Enforce Vendor Hold | ENFORCE_VENDOR_HOLD_FLAG |
| Notify if Blanket PO Exists | NOTIFY_IF_BLANKET_FLAG |
| RFQ Required | RFQ_REQUIRED_FLAG |
| Line Type | LINE_TYPE_ID |
| Allow Item Description Update | ALLOW_ITEM_DESC_UPDATE_FLAG |
| Display Disposition Messages | DISPOSITION_WARNING_FLAG |
| Enforce Full Lot Quantity | ENFORCE_FULL_LOT_QUANTITIES |
| Minimum Release Amount | MIN_RELEASE_AMOUNT |
| Price Type | PRICE_TYPE_LOOKUP_CODE |
| Price Break Type | PRICE_BREAK_LOOKUP_CODE |
| Receipt Close Point | RECEIVE_CLOSE_CODE |
| Invoice Close % | INVOICE_CLOSE_TOLERANCE |
| Receipt Close % | RECEIVE_CLOSE_TOLERANCE |
| Cancel Requisitions | CANCEL_REQS_ON_PO_CANCEL_FLAG |

| Setup Parameter Name | Column Name |
|---|-----------------------------|
| Requisition Import Group-By | REQIMPORT_GROUP_BY_CODE |
| Accrue Expense Items | EXPENSE_ACCRUAL_CODE |
| Accrue Inventory Items | INVENTORY_ACCRUAL_CODE |
| Order Type | ORDER_TYPE_ID |
| Order Source | ORDER_SOURCE_ID |
| Tax Default - Ship-To Location | TAX_FROM_SHIP_TO_LOC_FLAG |
| Tax Default - Item | TAX_FROM_ITEM_FLAG |
| Tax Default - Supplier | TAX_FROM_VENDOR_FLAG |
| Tax Default - Supplier Site | TAX_FROM_VENDOR_SITE_FLAG |
| Tax Default - Financial Options | TAX_FROM_SYSTEM_FLAG |
| Tax Default - Ship-To Location Hierarchy | TAX_HIER_SHIP_TO_LOC |
| Tax Default - Item Hierarchy | TAX_HIER_ITEM |
| Tax Default - Supplier Hierarchy | TAX_HIER_VENDOR |
| Tax Default - Supplier Site Hierarchy | TAX_HIER_VENDOR_SITE |
| Tax Default - Financial Options Hierarchy | TAX_HIER_SYSTEM |
| Enforce Price Tolerance Amount | ENFORCE_PRICE_CHANGE_AMOUNT |
| Price Tolerance Amount | PRICE_CHANGE_AMOUNT |

Setup Group Name: Receiving Options

Application: PO

Table Name: Rcv_Parameters

| Setup Parameter Name | Column Name |
|-----------------------------|--------------------------------|
| Over Receipt Tolerance % | QTY_RCV_TOLERANCE |
| Over Receipt Action | QTY_RCV_EXCEPTION_CODE |
| Enforce Ship-To | ENFORCE_SHIP_TO_LOCATION_CODE |
| Allow Express Transactions | ALLOW_EXPRESS_DELIVERY_FLAG |
| Receipt Date - Days Early | DAYS_EARLY_RECEIPT_ALLOWED |
| Receipt Date - Days Late | DAYS_LATE_RECEIPT_ALLOWED |
| Receipt Date - Action | RECEIPT_DAYS_EXCEPTION_CODE |
| Receipt Routing | RECEIVING_ROUTING_ID |
| Allow Substitute Receipts | ALLOW_SUBSTITUTE_RECEIPTS_FLAG |
| Allow Unordered Receipts | ALLOW_UNORDERED_RECEIPTS_FLAG |
| Allow Bind Receiving | BLIND_RECEIVING_FLAG |
| Receiving Inventory Account | RECEIVING_ACCOUNT_ID |
| Allow Cascade Transactions | ALLOW_CASCADE_TRANSACTIONS |
| ASN Control Action | RECEIPT_ASN_EXISTS_CODE |
| Receipt Number Action | USER_DEFINED_RECEIPT_NUM_CODE |
| Receipt Number Type | MANUAL_RECEIPT_NUM_TYPE |

Setup Group Name: Shipping Parameters

Application: WSH

Table Name: Wsh_Shipping_Parameters

| Setup Parameter Name | Column Name |
|-----------------------------------|-----------------------------|
| Goods Dispatched Account | GOODS_DISPATCHED_ACCOUNT |
| Weight UOM Class | WEIGHT_UOM_CLASS |
| Volume UOM Class | VOLUME_UOM_CLASS |
| Weight / Volume Calculation | WEIGHT_VOLUME_FLAG |
| Container Inventory Control | INV_CONTROLS_CONTAINER_FLAG |
| Percent Fill Basis | PERCENT_FILL_BASIS_FLAG |
| Default Delivery Document Set | DELIVERY_REPORT_SET_ID |
| Release Sequence Rule | PICK_SEQUENCE_RULE_ID |
| Pick Slip Grouping Rule | PICK_GROUPING_RULE_ID |
| Print Pick Slip | PRINT_PICK_SLIP_MODE |
| Default Pick Release Document Set | PICK_RELEASE_REPORT_SET_ID |

| Setup Parameter Name | Column Name |
|---|------------------------------|
| Autocreate Delivery Criteria | AUTOCREATE_DEL_ORDERS_FLAG |
| Default Stage Subinventory | DEFAULT_STAGE_SUBINVENTORY |
| Default Stage Locator | DEFAULT_STAGE_LOCATOR_ID |
| Auto Allocate | AUTODETAIL_PR_FLAG |
| Enforce Packing in Containers | ENFORCE_PACKING_FLAG |
| Group Delivery by Customer | GROUP_BY_CUSTOMER_FLAG |
| Group Delivery by FOB Code | GROUP_BY_FOB_FLAG |
| Group Delivery by Freight Terms | GROUP_BY_FREIGHT_TERMS_FLAG |
| Group Delivery by Intermediate Ship To Location | GROUP_BY_INTMED_SHIP_TO_FLAG |
| Group Delivery by Ship Method | GROUP_BY_SHIP_METHOD_FLAG |
| Number of Pick Slip Lines | PICK_SLIP_LINES |
| Autocreate Deliveries | AUTOCREATE_DELIVERIES_FLAG |
| Freight Class Category Set | FREIGHT_CLASS_CAT_SET_ID |
| Commodity Code Category Set | COMMODITY_CODE_CAT_SET_ID |
| Enforce Ship Sets and Ship Models | ENFORCE_SHIP_SET_AND_SMC |
| Defer Interface | DEFER_INTERFACE |
| Enforce Ship Method | ENFORCE_SHIP_METHOD |
| Allow Future Ship Date | ALLOW_FUTURE_SHIP_DATE |
| Secondary Export Country Screening | ITM_ADDITIONAL_COUNTRY_CODE |
| Auto Select Carrier | AUTO_SELECT_CARRIER |
| Ship Confirm Rule | SHIP_CONFIRM_RULE_ID |
| Autopack Delivery | AUTOPACK_LEVEL |
| Plan Tasks | TASK_PLANNING_FLAG |

Setup Group Name: Assets System Controls

Application: FA

Table Name: Fa_System_Controls

| Setup Parameter Name | Column Name |
|---|--------------------------|
| Enterprise Name | COMPANY_NAME |
| Oldest Date Placed In Service | DATE_PLACED_IN_SERVICE |
| Starting Asset Number | INITIAL_ASSET_ID |
| Location Flexfield | LOCATION_FLEX_STRUCTURE |
| Category Flexfield | CATEGORY_FLEX_STRUCTURE |
| Asset Key Flexfield | ASSET_KEY_FLEX_STRUCTURE |
| Accept Assets With Start Date Before Parent | CUA_INHERITANCE_FLAG |

Setup Group Name: Federal Options

Application: FV

Table Name: Fv_Federal_Options

| Setup Parameter Name | Column Name |
|-----------------------------------|------------------------|
| Asset Discount Transaction Code | DISC_TRAN_CODE_ASSET |
| Expense Discount Transaction Code | DISC_TRAN_CODE_EXPENSE |

Setup Group Name: Federal System Parameters

Application: FV

Table Name: Fv_System_Parameters

| Setup Parameter Name | Column Name |
|--|--------------------------------|
| Customer Trading Partner | FACTSI_CUSTOMER_ATTRIBUTE |
| Vendor Trading Partner | FACTSI_VENDOR_ATTRIBUTE |
| Adjustment Status | REP_2209_ATTRIBUTE |
| Journal Trading Partner | FACTSI_JOURNAL_ATTRIBUTE |
| Project Accounting Accomplished Date | SF224_ACCOMPLISH_DATE |
| Public Law Code | FACTSII_PUB_LAW_CODE_ATTRIBUTE |
| Advance Type | FACTSII_ADVANCE_TYPE_ATTRIBUTE |
| Transfer - Main Account | FACTSII_TR_MAIN_ACCT_ATTRIBUTE |
| Transfer - Department ID | FACTSII_TR_DEPT_ID_ATTRIBUTE |
| Requisition Transaction Date | REQ_DATE_SEG |
| Purchase Order Transaction Date | PUR_ORDER_DATE_SEG |
| Receiving Transaction Date | REC_TRXN_DATE_SEG |
| Adjustment To Invoice Paid In Prior Year | PYA_INVOICE_ATTRIBUTE |

