GRC300

SAP BusinessObjects Access Control 10.0 - Implementation and Configuration

COURSE OUTLINE

Course Version: 15
Course Duration: 5 Day(s)
SAP Copyrights and Trademarks

© 2017 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. Please see http://global12.sap.com/corporate-en/legal/copyright/index.epx for additional trademark information and notices.

Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors.

National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP SE or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP SE or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE’s or its affiliated companies’ strategy and possible future developments, products, and/or platform directions and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, which speak only as of their dates, and they should not be relied upon in making purchasing decisions.
American English is the standard used in this handbook. The following typographic conventions are also used.

<table>
<thead>
<tr>
<th>Typographic Convention</th>
<th>Illustration</th>
</tr>
</thead>
<tbody>
<tr>
<td>This information is displayed in the instructor’s presentation</td>
<td>![Display Icon]</td>
</tr>
<tr>
<td>Demonstration</td>
<td>![Down Arrow]</td>
</tr>
<tr>
<td>Procedure</td>
<td>![Steps]</td>
</tr>
<tr>
<td>Warning or Caution</td>
<td>![Exclamation Point]</td>
</tr>
<tr>
<td>Hint</td>
<td>![Light Bulb]</td>
</tr>
<tr>
<td>Related or Additional Information</td>
<td>![Forward Arrow]</td>
</tr>
<tr>
<td>Facilitated Discussion</td>
<td>![Chat Bubbles]</td>
</tr>
<tr>
<td>User interface control</td>
<td><em>Example text</em></td>
</tr>
<tr>
<td>Window title</td>
<td><em>Example text</em></td>
</tr>
</tbody>
</table>
# Contents

<table>
<thead>
<tr>
<th>Unit</th>
<th>Topic</th>
<th>Lessons</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>Unit 1: Introduction to SAP Access Control</strong></td>
<td>Lesson: Discussing Business Challenges and Solutions</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lesson: Using SAP Access Control</td>
</tr>
<tr>
<td>3</td>
<td><strong>Unit 2: Architecture, Security, and Authorizations</strong></td>
<td>Lesson: Describing the System Architecture</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lesson: Describing Security and Authorizations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lesson: Managing Risk by Segregating Duties</td>
</tr>
<tr>
<td>7</td>
<td><strong>Unit 4: Shared Configuration Settings</strong></td>
<td>Lesson: Configuring Shared GRC Settings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lesson: Configuring Shared Access Control Settings</td>
</tr>
<tr>
<td>9</td>
<td><strong>Unit 5: Access Control Repository</strong></td>
<td>Lesson: Synchronizing Objects into the Repository</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lesson: Scheduling and Viewing Background Jobs</td>
</tr>
<tr>
<td>11</td>
<td><strong>Unit 6: Business Rule Framework</strong></td>
<td>Lesson: Creating Rules in the Business Rule Framework (BRF)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lesson: Defining Business Rules</td>
</tr>
<tr>
<td>13</td>
<td><strong>Unit 7: MSMP Workflow</strong></td>
<td>Lesson: Describing Multi-Stage Multi-Path (MSMP) Workflow</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lesson: Maintaining MSMP Workflow: Part One</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lesson: Maintaining MSMP Workflow: Part Two</td>
</tr>
<tr>
<td>15</td>
<td><strong>Unit 8: Analyze and Manage Risk</strong></td>
<td>Lesson: Maintaining Shared Master Data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lesson: Configuring and Maintaining the Rule Set</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lesson: Using and Configuring Audit Trail Tracking</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lesson: Using the Risk Analysis Framework</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lesson: Remediating Risks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lesson: Mitigating Risks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lesson: Mass Mitigating</td>
</tr>
<tr>
<td>Unit</td>
<td>Number</td>
<td>Title</td>
</tr>
<tr>
<td>------</td>
<td>--------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>10</td>
<td>19</td>
<td>Design and Manage Roles</td>
</tr>
<tr>
<td>13</td>
<td>25</td>
<td>Reports and Custom Fields</td>
</tr>
<tr>
<td>14</td>
<td>27</td>
<td>SAP Access Control Implementation</td>
</tr>
</tbody>
</table>
Course Overview

TARGET AUDIENCE
This course is intended for the following audiences:

• Data Consultant
• Development Consultant
• Industry / Business Analyst Consultant
• Support Consultant
• Technology Consultant
• Project Stakeholder
• System Administrator
• IT Support
• Super / Key / Power User
Lesson 1: Discussing Business Challenges and Solutions

Lesson Objectives
After completing this lesson, you will be able to:

- Describe business challenges and process integrations
- Discuss solution harmonization concepts

Lesson 2: Using SAP Access Control

Lesson Objectives
After completing this lesson, you will be able to:

- Navigate the user interface and describe work center functionality
Lesson 1: Describing the System Architecture

Lesson Objectives
After completing this lesson, you will be able to:

- Describe the SAP GRC architecture and landscape
- Describe the SAP Access Control 10.0 Architecture

Lesson 2: Describing Security and Authorizations

Lesson Objectives
After completing this lesson, you will be able to:

- Describe object-level security, authorization requirements and delivered roles
UNIT 3

Authorization Risks and the SoD Management Process

Lesson 1: Identifying Authorization Risks

Lesson Objectives
After completing this lesson, you will be able to:

- Identify authorization risks in the Purchase-to-Pay process
- Identify the risk of a person adjusting and approving payroll

Lesson 2: Managing Risk by Segregating Duties

Lesson Objectives
After completing this lesson, you will be able to:

- Describe the main SoD Risk Management process and the roles that are involved to identify and resolve SoD issues
- Identify and classify risks during Phase One of the SoD Risk Management Process
- Describe SoD Risk Management Process Phase One, Step Two tasks: Rule building components and the delivered rule set
- Describe the steps for Phase Two of the SoD Risk Management process: Analysis, Remediation, and Mitigation
- Describe the tasks of Phase Three of the SoD Risk Management process to maintain ongoing compliance
Lesson 1: Configuring Shared GRC Settings

Lesson Objectives
After completing this lesson, you will be able to:

- Configure the Integration Framework

Lesson 2: Configuring Shared Access Control Settings

Lesson Objectives
After completing this lesson, you will be able to:

- Configure shared SAP Access Control settings
- Identify Business Configuration (BC) Sets
Lesson 1: Synchronizing Objects into the Repository

Lesson Objectives
After completing this lesson, you will be able to:

- Describe the SAP Access Control Repository and order of jobs
- Synchronize PFCG Authorization Data
- Synchronize profile, role, and user data
- Synchronize usage types into the SAP Access Control Repository

Lesson 2: Scheduling and Viewing Background Jobs

Lesson Objectives
After completing this lesson, you will be able to:

- Schedule background jobs
- View background jobs
Lesson 1: Creating Rules in the Business Rule Framework (BRF)

Lesson Objectives
After completing this lesson, you will be able to:

- Discuss BRMS (Business Rules Management Systems) and BRFplus concepts
- Define workflow-related MSMP rules

Lesson 2: Defining Business Rules

Lesson Objectives
After completing this lesson, you will be able to:

- Create rules using the BRFplus workbench
Lesson 1: Describing Multi-Stage Multi-Path (MSMP) Workflow

Lesson Objectives
After completing this lesson, you will be able to:

- Describe MSMP workflow and configuration prerequisites
- Describe the main steps of the MSMP Workflow process

Lesson 2: Maintaining MSMP Workflow: Part One

Lesson Objectives
After completing this lesson, you will be able to:

- Configure Process Global Settings
- Maintain rules for MSMP workflow
- Maintain agents for MSMP Workflow
- Maintain Notification Variables and Templates
- Maintain paths and stages for MSMP workflow

Lesson 3: Maintaining MSMP Workflow: Part Two

Lesson Objectives
After completing this lesson, you will be able to:

- Map workflow routings
- Generate versions for MSMP Workflow
Lesson 1: Maintaining Shared Master Data

Lesson Objectives
After completing this lesson, you will be able to:

- Maintain shared organizations and organization views
- Describe how mitigating controls are shared and centrally assign owners

Lesson 2: Configuring and Maintaining the Rule Set

Lesson Objectives
After completing this lesson, you will be able to:

- Configure Access Risk Analysis
- Maintain Access Rules
- Describe the workflow process for function maintenance
- Maintain Risks and Critical Access Rules
- Execute and monitor batch risk analysis

Lesson 3: Using and Configuring Audit Trail Tracking

Lesson Objectives
After completing this lesson, you will be able to:

- Configure and track audit trails

Lesson 4: Using the Risk Analysis Framework

Lesson Objectives
After completing this lesson, you will be able to:

- Perform risk analysis and dynamically customize analysis results

Lesson 5: Remediating Risks

Lesson Objectives
After completing this lesson, you will be able to:

- Develop a risk remediation strategy

Lesson 6: Mitigating Risks

Lesson Objectives
After completing this lesson, you will be able to:

- Mitigate risks on specific systems
- Create mitigating controls and assignments on specific systems

Lesson 7: Mass Mitigating

Lesson Objectives
After completing this lesson, you will be able to:

- Mitigate large numbers of risks at one time
Lesson 1: Managing Emergency Access

Lesson Objectives
After completing this lesson, you will be able to:

• Describe Emergency Access architecture and maintenance tasks
• Perform firefighting on multiple client systems from a single console

Lesson 2: Planning for Emergency Access

Lesson Objectives
After completing this lesson, you will be able to:

• Identify critical firefighting roles and assignments
• Maintain and Assign Firefighter IDs
• Maintain firefighting reason codes and track reason code usage

Lesson 3: Monitoring Emergency Access

Lesson Objectives
After completing this lesson, you will be able to:

• Use firefighting reports to view session details, reason codes, and activity
• Use the Log Collector to fetch firefighting-related logs
• Use the Consolidated Log Report to segment or combine collected logs
Lesson 1: Configuring Role Management

Lesson Objectives
After completing this lesson, you will be able to:

- Describe configuration options specific to designing and managing roles

Lesson 2: Configuring Role Methodology

Lesson Objectives
After completing this lesson, you will be able to:

- Configure Role Creation Methodology
- Configure a BRFplus rule for role methodology and approvers
- Assign Condition Group Type to BRFplus Application and Function
- Define Role Methodology process and steps
- Associate role methodology process to condition group

Lesson 3: Planning for Technical Role Definition

Lesson Objectives
After completing this lesson, you will be able to:

- Define single roles (technical roles) and role mapping
- Document CUA Composite Roles and manage role authorizations

Lesson 4: Planning for Business Role Definition

Lesson Objectives
After completing this lesson, you will be able to:

- Define business roles

Lesson 5: Consolidating Roles through Role Mining

Lesson Objectives
After completing this lesson, you will be able to:

- Compare role authorizations and definitions, and view transaction usage
- Certify role content periodically

**Lesson 6: Mass Managing Roles**

**Lesson Objectives**

After completing this lesson, you will be able to:

- Mass manage roles
Lesson 1: Defining User Provisioning
Lesson Objectives
After completing this lesson, you will be able to:
- Configure settings to provision users

Lesson 2: Designing End User Personalization Forms
Lesson Objectives
After completing this lesson, you will be able to:
- Configure end user personalization forms and access request templates

Lesson 3: Planning for User Access
Lesson Objectives
After completing this lesson, you will be able to:
- Create a user access request
- Create an access request with a model user
- Create an access request with a template
- Create an access request from a copy
- Request an Organizational Assignment

Lesson 4: Requesting User Access Approval
Lesson Objectives
After completing this lesson, you will be able to:
- Describe user access approval concepts and configuration settings
- Respond to access requests and review the audit log
Lesson 1: Planning Periodic Review

Lesson Objectives
After completing this lesson, you will be able to:

- Configure parameters for Periodic Access Review Requests

Lesson 2: Monitoring Periodic Review

Lesson Objectives
After completing this lesson, you will be able to:

- Review user access risk using SoD review
- Periodically reaffirm roles
Lesson 1: Working with the Reporting Framework

Lesson Objectives

After completing this lesson, you will be able to:

- Change an existing report without programming
- Add custom fields to a report
Lesson 1: Working with the Access Control Implementation Process

Lesson Objectives
After completing this lesson, you will be able to:

• Describe the main implementation steps and project team members

Lesson 2: Designing the Access Control Solution

Lesson Objectives
After completing this lesson, you will be able to:

• Design the SAP Access Control Solution

Lesson 3: Planning Upgrade and Migration

Lesson Objectives
After completing this lesson, you will be able to:

• Identify key considerations for upgrade and migration

Lesson 4: Configuring Access Control

Lesson Objectives
After completing this lesson, you will be able to:

• Perform final tasks and prepare for go live

Lesson 5: Implementing the Solution

Lesson Objectives
After completing this lesson, you will be able to:

• Perform final tasks and prepare for go live

Lesson 6: Optimizing and Enhancing the Solution

Lesson Objectives
After completing this lesson, you will be able to:

- Ensure system stability and optimize performance