SAP SECURITY ADMINISTRATION TRAINING PROGRAM (ECC-GRC 1.0 (AC) BW/BI and HR Security.

1. Overview of SAP
2. Introduction to SAP Security
3. Implementation methodology

1). USER ADMINISTRATION

Single User administration

1. New Hire Policy (On-Boarding Process)
2. Termination Policy
3. Single User Creation
4. user Deletion
5. Single User Lock
6. Single User Unlock
7. Single User password change
8. Setting Single User validity
9. Copying Existing user to new user
10. Comparing two users:

Mass User administration

11. Mass User Creation
12. Mass User deletion
13. Mass User Lock
14. Mass User Unlock
15. Setting up validity for mass users
16. Locking the users using EWZ5

LSMW:

CUA (Central User administration)

Working with USR* Tables for Auditing Purpose

2). ROLE ADMINISTRATION

1. Types of Role
2. Implementation of Master-Derived Role Strategy
3. Implementation of Single-Composite Role Strategy
4. Working with Check Indicators and Proposal Values
5. Status of Authorization Objects
6. Creating Single Role
7. Creating Composite Role
8. Creating Derived Role
9. Assigning Single Role to Multiple Users
10. Assigning Multiple Roles to Single User
11. Assigning Multiple Roles to Multiple Users

12. Deleting T_Code from an Existing Role
13. Adding T_Code to an Existing Role
14. Deleting a Role
15. Single Role Transportation
16. Multiple Role Transportation
17. Deleting Inheritence between parent & child Roles
18. Single Role Download & Upload
19. Mass Role Download & Upload
20. User Comparison
21. Setting up role validity
22. Copying Role as it is
23. Copying Role with selected options
24. Importing roles from another system using RFC
25. Comparing Two Roles with in the system

3). Transporting Role across Landscape from DEV QAS PRD
4). Transporting Role across System from one client to another
5). Authorization Group Concept
6). Display Missing Authorization Values
7). System Trace
8). Authorization Information System
9).Auditing And Logging Security Policy

1. Security Audit Log Configuration
2. Displaying Security Audit Log

10). Tables for User and Role admin

1. Working with RSUSR* Programs for Auditing Purpose
2. Working with USR* Tables for Auditing Purpose
3. Working with AGR* Tables for Auditing Purpose
4. Working with ADR* Tables for Auditing Purpose

SAP BUSINESS OBJECTS GOVERNANCE RISK COMPLIANCE ACCESS CONTROL 10.0 CONTENT

GRC GENERIC SETTINGS

- Pre-assembled Deployment Scenario
- Prerequisites
- Manual Check
- Allowing Crystal Reports
- Activating the Applications in Clients
- Setting Decimal Notation and Date Format
- Updating BC Set Definitions
- Checking Logon Language
- Maintaining Client Settings
- Setting up Transport Connection
- Active Workflow
- Performing Automatic Workflow Customizing
- Common Component Settings
- Maintaining Connectors and Connection Types
- Shared Master Data Settings
- Creating Root Organization Hierarchy

ACCESS CONTROL GENERIC SETTINGS

- Pre-assembled Deployment Scenario
- Configuration
- Integration Framework - Maintain Connection Settings
- Maintaining Configuration Settings
- Maintaining Connector Settings
- Maintaining Mapping for Actions and Connector Groups
- Maintaining Business Processes and Sub-processes
- Maintaining Data Sources Configuration
- Maintaining Project and Product Release Name
- Master Data – SAP GUI
- Checking Required Users in ERP Target System
- Creating Users in GRC System
- Generating SoD Rules
- Synchronization Jobs
- Workflow for Access Control
- Master Data – SAP NWBC
- Assigning Access Owner – Role Owner
- Mass Role Import

ACCESS RISK MANAGEMENT

- Pre-assembled Deployment Scenario
- Configuration – SAP NWBC
- Assigning Access Control Owner
- Assigning MC Approver/Monitor to Organization Owner
- Creating Mitigating Control for Risk P004, S003
- Maintaining UAR/SoD Review Coordinators
- Maintaining Risk Owners to Risks
- Configuration – SAP GUI
- Checking Workflow Templates Activation Status
- Setting Task to General Task
- Email Notification for Mitigation Control Maintenance Workflow
- Generating MSMP Process Versions
- Synchronizing Profiles in Repository
- Synchronizing Roles in Repository
- Synchronizing Users/Roles Used by Users
- Retrieving Role Usage
- Executing Batch Risk Analysis – Initial Run
- Executing Batch Risk Analysis - Regular Run
- Monitoring Batch Risk Analysis
- Enabling Mitigating Control Workflow
- Maintaining Custom User Group for Scenario Users

ACCESS REQUEST MANAGEMENT

- Prerequisites
- Configuration
- Pre-assembled Deployment Scenario
- Checking Workflow Templates Activation Status
- Setting Task to General Task
- Maintaining MSMP Workflow
- Defining Business Rule Framework For User Access
- Maintaining Approvers
- Maintaining Rules
- Maintaining Agents
- Maintaining Stages
- Maintaining Process Initiator
- Maintaining Paths for Process
- Assigning Stages to Path
- Maintaining Stage Notification Settings
- Maintaining Route Mapping

- Maintaining Process Escape Conditions
- Generating MSMP Process Versions
- Assigning Access Control Owners
- Assigning Firefighter Owner to Firefighter ID
- Assigning Firefighter Controller to Firefighter ID
- Creating Reason Codes
- Active Audit Review Workflow
- Checking Workflow Templates Activation Status
- Setting Task to General Task
- Generating MSMP Process Versions
- Decentralized Firefighting Settings
- EAM Master Data Sync - Initial Run
- EAM Master Data Sync - Regular Run
- Maintaining Configuration Settings (SAP ERP)
- Maintaining Custom Notification Messages for Emergency Access (SAP ERP)

EMERGENCY ACCESS MANAGEMENT

Purpose

Prerequisites

- Roles
- Overview Table
- Test Procedures

Centralized EAM

- Requesting for Firefighter ID
- Request Approved by Firefighter Owner
- Using Firefighter ID Logon (SAP AC)
- Starting Firefighter Session (SAP ERP)
- Reviewing and Approving the Firefighter Log
- Reviewing Consolidated Log Report

Decentralized EAM

- Requesting for Firefighter ID (Optional)
- Request Approved by Firefighter Owner (Optional)
- Using Firefighter ID Logon (SAP ERP)
- Starting Firefighter Session (SAP ERP)
- Reviewing and Approving the Firefighter Log
- Reviewing Consolidated Log Report
- Reverse Steps

- Reversal of Process Steps

BW/BI Security:

1. Introduction to BW/BI Systems.
2. Info Providers- Info Objects, Info Cubes, Multi Provider,
3. Restricting Access to Info provider.
4. Trouble shooting BW/BI Authorizations.
5. BW/BI Related Authorization Objects.
6. Types of BW Users.
7. Analysis Authorization (AA) Concept.
8. Trouble shooting AA access
9. Replicating Users in Access issues.
10. BW/BI Related Tables.

HR Security:

1. Introduction HR Security.
2. Over view of HR Data.
3. Info types and Sub Types.
4. Authorization restriction based on Info Types.
5. HR Objects, Positions, Org Units, Cost centers, Personal Number etc…
6. Indirect role assignment.
7. Structural Authorization concept.
8. Security T-codes and Objects.
9. PD Profiles creation.
10. Organization assignment to PD Profiles.
11. HR Related Tables.
12. Trouble shooting HR access

Pre-requisite: SAP Security Consultant Work Experience or SAP Security Trained Candidates only Eligible for this Training.