



SAP Security and GRC

SAP SECURITY :

INTRODUCTION TO SAP & SAP SECURITY

- What is SAP & Why?
- What is Security & Why?
- Landscape
- Transaction codes

USER ADMINISTRATION.

- Single user creation SU01
- Create user
- Reset/Change/Deactivate Password
- Assign Roles/Profiles.
- Lock /Unlock user
- Delete user
- Mass user creation SU10
- Create users
- Deactivate mass users password
- Assign Roles/profiles
- Lock / unlock users
- Delete mass users
- Disadvantages of SU10
- User types and uses
- User groups.
- Central user administration (CUA).

ROLE ADMINISTRATION.

- Concept of Roles
- Role types
- Single role
- Composite role
- Master/Template role
- Derived role
- Parent Role & Child Role.
- Introduction to Authorization objects
- Authorization Objects.
- Activities/fields.
- Authorization profiles.
- Programming authorizations.



VtechSoft

Solutions

- Important Authorization objects
- Add manually authorization objects/T-codes.
- Deactivate authorization object.

ROLE TRANSPORT.

- Transport request types
- Transport single /mass roles.
- Release transport
- Import transport.
- Role Download/upload.
-

USER information (SUIM).

- User selection criteria
- Roles by complex selection criteria.
- Comparison.
- Change documents

RESTRICTION ON TABLES.

- Authorization group creation.
- Map authorization group to Tables.

TROUBLESHOOTING.

- SU53 - Missing Authorizations
- ST01 - Authorization Trace

CHECK INDICATOR /SU24 CHANGES.

- Types of Authorization Status
- Importance of customer tables.



BI-SECURITY

- Architecture and strategies for a BI authorization concept
- Security requirements in SAP BI
- Standard roles and templates for the authorization concept
- Creating BW/BI roles and modification
- Difference between BW and R/3 security
- Difference between BW and BI Security
- Different authorization objects involved in BW/BI
- Analysis authorization concept and reporting
- Troubleshooting BW/BI issues

HR-SECURITY

- Structural authorizations
- HR Master Data authorizations
- Authorization main switches
- Authorization objects for payroll
- Info types concept
- Tables in HR

GRC10.0

- Architecture & features of GRC 10.0
- Difference between GRC5.3 & GRC 10.0
- Migration steps from GRC5.3 to GRC10.0
- Installation steps of GRC10.0
- Post installation activities of GRC10.0
- Introduction on new components in GRC10.0

ARA (ACCESS RISK ANALYSIS)

- What is Risk
- SoD Checks and rule book
- Configuring and Maintaining the Rule Set
- Analyze and Manage Risk
- Maintain a Critical Access Rule
- Role Level Simulation
- User Level Simulation
- Perform Ad Hoc Risk Analysis
- Mitigating Risks



EAM (EMERGENCY ACCESS MANAGEMENT)

- Emergency Access Management Configuration
- Maintain Owners and Controllers in Central Owner Maintenance
- Assign Owners to Firefighter IDs
- Assign Controllers to Firefighter IDs
- Assign Firefighter Users to Firefighter IDs
- Maintain Reason Codes
- Monitoring Emergency Access
- Review a Log Report

ARM (ACCESS REQUEST MANAGEMENT)

- Business Rules Framework
- Maintaining MSMP Workflow
- Customize Workflow
- Settings Specific to Provisioning and Managing Users
- End User Personalization Forms
- Create an Access Request

BRM (BUSINESS ROLE MANAGEMENT)

- Configuring Role Management
- Roles-Specific Configuration Options
- Configuring Role Methodology
- Settings for Condition Groups