GRC&SECURITY

Course curriculum:

We have segregated SAP Security training in different categories like User Administration, Role Administration, Troubleshooting, Audit Compliance Reporting and Other Key activities

What is SAP and how it works:

- Introduction to ERP
- Get an overview of SAP R/3
- About various SAP Versions
- Introduction to SAP Security
- Why we need security
- What needs to be secured

User Administration:

- User lock/unlocking and Resetting Password
- User creation – IT users and Business users
- Different type of users in SAP
- Creation of RFC,BATCH and OSS users
- User Groups creation
- Significance of user groups and maintenance
- Significance of Parameters and maintenance
- Role assignment/removal on temporary basis and permanent basis
- Mass maintenance of user access
- Extending user validity and extending role validity
- User inactivation and user reactivation
- User termination
- Usage data – STAD and SM20(Audit log)
- Transaction lock and unlock
- User Information System for different kind of reports

Flat No: 506,5th Floor, Nilgiri Block, Aditya Enclave, Ameerpet ,Hyd -5000038.
Contact: +91 9032734343, Mail: info@vritsol.com www.vritsol.com

- Central User Administration

Role Administration:

- Understanding SAP Authorization Concept
- Role Naming Conventions for different type of roles
- Creation of single roles
- Creation of composite Roles
- Creation of master and derived roles
- Adding/Removing Tcode from roles
- Creation of global roles
- SU22 and SU24 - Understanding Concept
- Modifying SU24 check indicators
- Role transportation
- Template role creation
- Area menu role creation
- Role upload and download

Troubleshooting Access issues:

- Understanding of SU53 for missing authorizations
- Finding suitable roles with SU53 and providing missing access to users
- Tracing authorizations issues with ST01
- Updating objects in the roles as per missing authorizations
- Updating organizational values in roles
- Restriction of table and program level access

Other Key Activities:

- Client open procedures for configuration changes and coordination with Basis team
- OSS Access details updating in service market place
- Developer key and Object key generation in service market place
- SAP Licensing(Measurement Data)
- Providing sensitive Tcode, objects and Roles access
- CATT scripting for various mass process
- Change Management Process
- System validations from Security in maintenance activities
- Approval Process
- Ticketing tools
- SLAs
- Different SAP Security tables and usage in real time

SAP Security Reporting for Audit Compliance:

- What is SOX and SOD
- Down loading user's report who are not login to the system from past 90 days
- Client Settings status
- Security System Parameter checking
- Forbidden Password Report
- Tracking security users list and their roles
- Random request checking for quality checking
- User termination as per weekly HR termination report
- List the non dialog users and make sure those users should not be in locked status
- Download SM20-audit log report on weekly basis
- Users with Incomplete Address Data
- SAP_ALL & SAP_NEW assignment review
- Protection of SAP Standard users

- Document detail steps of debug/critical access

BI Security:

- Architecture and strategies for a BI authorization concept
- Difference between BI and ECC security
- Security Design and Approach
- Role structure in BI Security
- Different authorization objects involved in BI
- Analysis Authorization creation and maintenance
- Troubleshooting analysis authorization issues

****

SAP GRC 10.1 Access Controls

- Introduction of GRC and other compliance tools
- Introduction of SOX Rules and SOD Concept Explanation
- Key Features and Benefits
- GRC Architecture and Landscape
- Brief Overview of SAP Users and Authorizations
- Describing Tcode level and Object-Level Security

Shared configuration settings

- Configure the Integration Frame work including connector setup
- Configure shared Access Control Settings
- Identify Business Configuration (BC) sets
- Importance of NWBC
- Different type of GRC AC roles

Access Risk Analysis- ARA (Earlier RAR)

- Verifying default configuration parameters

- Adding connector to AUTH scenario
- Generating rules
- Synchronizing authorizations
- Synchronizing repository
- Explanation on Functions, Risks and Rules
- Risk Analysis framework and types
- Risk Analysis Simulation
- Remediating Risks
- Mitigating Risks
- Mass Mitigating
- Different types of background jobs in ARA
- Setting up rule sets

Emergency Access Management - EAM (Earlier SPM-FF)

- Configuring EAM and importance of EAM configuration parameters
- Centralized Firefighting
- Creating different users and assigning roles
- Fire Fighting Types - ID based and Role based
- Managing Emergency Access
- Planning for Emergency Access
- Assigning OWNER and CONTROLLER to FF ID
- Checking FF logs
- Maintain Reason Codes
- Background jobs in EAM
- Audit Reports

Access Request Management - ARM (Earlier CUP)

- Creating Access Request

- Types of Access requests
- Requesting User Access Approval
- Responding to Access Requests
- Audit log
- Defining User Provisioning
- Describing Multi-Stage Multi-Path Workflow
- Maintaining MSMP Workflow
- BRF+ Workflow setup
- Monitor User Access
- Role Import
- Password self-service [PSS]

Business Role Management –BRM (Earlier ERM)

- Configuring Role Management
- Configuring Role Methodology
- Activating required BC sets
- Technical Role definition
- Workflow setup
- Creation of roles with BRM