

SAP GRC Access Control

COURSE CONTENT

GET IN TOUCH



Multisoft Systems
B - 125, Sector - 2, Noida



(+91) 9810-306-956



info@multosoftsystems.com



www.multosoftsystems.com

About Multisoft

Train yourself with the best and develop valuable in-demand skills with Multisoft Systems. A leading certification training provider, Multisoft collaborates with top technologies to bring world-class one-on-one and certification trainings. With the goal to empower professionals and business across the globe, we offer more than 1500 training courses, which are delivered by Multisoft's global subject matter experts. We offer tailored corporate training; project Based Training, comprehensive learning solution with lifetime e-learning access, after training support and globally recognized training certificates.

About Course

SAP GRC Access Control Training is designed to help professionals understand how access governance, segregation of duties control, privileged access monitoring, and user access management are handled across SAP environments. The course covers Access Risk Analysis, Access Request Management, Emergency Access Management, Business Role Management, mitigating controls, and compliance monitoring. Participants will gain practical knowledge of how to identify access risks, manage user and role governance, support audit requirements, and strengthen SAP security through structured access control and compliance processes.

Module 1: Introduction to SAP GRC Access Control

- ✓ Overview of SAP GRC and Access Governance
- ✓ Role of SAP GRC Access Control in SAP Security
- ✓ Key Components of SAP GRC Access Control
- ✓ Access Governance and Compliance Concepts
- ✓ SAP GRC Access Control Architecture
- ✓ Business Benefits and Use Cases

Module 2: SAP GRC Access Control Foundation and System Landscape

- ✓ SAP GRC Landscape Overview
- ✓ Connected Systems and Integration Concepts
- ✓ User, Role, and Authorization Basics in SAP
- ✓ Access Control Configuration Foundations
- ✓ System Connectors and Landscape Considerations
- ✓ Organizational Roles in Access Governance

Module 3: Access Risk Analysis (ARA) Fundamentals

- ✓ Introduction to Access Risk Analysis
- ✓ Segregation of Duties (SoD) Concepts
- ✓ Critical Access and Sensitive Access Risks
- ✓ User-Level and Role-Level Risk Analysis
- ✓ Risk Identification and Risk Categorization

- ✓ Business Importance of ARA

Module 4: Access Risk Analysis Configuration and Execution

- ✓ Risk Rule Set Concepts
- ✓ Function, Action, and Permission Mapping
- ✓ Risk Analysis for Users, Roles, Profiles, and HR Objects
- ✓ Batch Risk Analysis and Simulation
- ✓ Risk Analysis Reports and Interpretation
- ✓ Risk Remediation Planning

Module 5: Mitigating Controls and Compliance Management

- ✓ Purpose of Mitigating Controls
- ✓ Mitigation Control Definition and Assignment
- ✓ Control Ownership and Approval
- ✓ Linking Controls to Risks and Users
- ✓ Monitoring Mitigation Effectiveness
- ✓ Compliance and Audit Support Processes

Module 6: Emergency Access Management (EAM)

- ✓ Firefighter ID and Emergency Access Concepts
- ✓ EAM Architecture and Components

- ✓ Firefighter User Setup and Role Assignment
- ✓ Firefighter Log Review Process
- ✓ Emergency Access Monitoring and Control
- ✓ Compliance Requirements for Privileged Access

Module 7: Access Request Management (ARM)

- ✓ Access Request Management Overview
- ✓ Request Types and Access Request Lifecycle
- ✓ User Provisioning Requests
- ✓ Role and Access Assignment Requests
- ✓ Approval Workflow Structure
- ✓ Request Validation and Processing

Module 8: ARM Workflow, Provisioning, and Request Controls

- ✓ ARM Workflow Configuration Concepts
- ✓ Stage Approvals and Multi-Level Approval Routing
- ✓ Provisioning Integration Concepts
- ✓ Risk Check During Request Submission
- ✓ Request Rejection, Modification, and Escalation
- ✓ Monitoring Request Processing

Module 9: Business Role Management (BRM)

- ✓ Introduction to Business Role Management
- ✓ Role Lifecycle Management Concepts
- ✓ Role Creation, Ownership, and Approval
- ✓ Role Maintenance and Version Control
- ✓ Business Roles vs Technical Roles
- ✓ Role Governance Best Practices

Module 10: User Provisioning and Access Governance Operations

- ✓ User Provisioning Process Overview
- ✓ Access Assignment Governance
- ✓ Role Provisioning and De-Provisioning Concepts
- ✓ Joiner-Mover-Leaver Access Governance Considerations
- ✓ Monitoring Access Changes
- ✓ Operational Access Governance Practices

Module 11: Reporting, Dashboards, and Monitoring

- ✓ SAP GRC Access Control Reporting Framework
- ✓ Access Risk Reports
- ✓ SoD Analysis Reports
- ✓ Firefighter and EAM Monitoring Reports

- ✓ ARM and Request Tracking Reports
- ✓ Compliance Dashboards and Monitoring Views

Module 12: Audit Readiness and Compliance Support

- ✓ Access Governance for Internal and External Audits
- ✓ Supporting Audit Evidence with SAP GRC
- ✓ Review of Access Logs and Control Records
- ✓ Periodic Access Review Considerations
- ✓ Compliance Documentation and Traceability
- ✓ Governance Best Practices for Audit Readiness

Module 13: Administration, Best Practices, and Operational Support

- ✓ Administrative Responsibilities in SAP GRC Access Control
- ✓ Master Data and Rule Maintenance Considerations
- ✓ Operational Monitoring and Support Activities
- ✓ Common Access Governance Challenges
- ✓ Troubleshooting Access Control Processes
- ✓ Best Practices for Stable SAP GRC Operations

Module 14: Real-World Scenarios and Implementation Use Cases

- ✓ SoD Conflict Analysis Scenarios
- ✓ Emergency Access Governance Use Cases
- ✓ Access Request and Approval Scenarios
- ✓ Role Governance Examples
- ✓ Compliance and Audit Support Use Cases
- ✓ End-to-End SAP GRC Access Control Process Walkthroughs