



GLOSSARY OF SAP S/4HANA GRC ACCESS CONTROL

**A Quick Reference Guide to
SAP Terminologies**

Concept/Term	Definition
SAP GRC (Governance, Risk, and Compliance)	A suite of tools in SAP designed to manage enterprise governance, mitigate risk, and ensure compliance across business processes.
Access Control (AC)	A module within SAP GRC that manages user access to SAP systems, ensuring that employees only have the permissions they need to perform their job duties.
Segregation of Duties (SoD)	The practice of ensuring that no one individual has the ability to perform conflicting duties within SAP, reducing the risk of fraud or error.
Access Risk Analysis (ARA)	A process in SAP GRC that identifies and analyzes risks associated with user access to ensure compliance and reduce SoD violations.
Access Request Management (ARM)	A feature in SAP GRC that allows users to request access to SAP systems, which is then reviewed and approved or rejected by authorized personnel.

Concept/Term	Definition
Role Management	The process of creating, maintaining, and assigning roles to users, defining access permissions based on job functions within the SAP system.
User Provisioning	The process of creating, managing, and deactivating user accounts and assigning appropriate access roles and permissions in SAP systems.
Compliance Management	The practice of ensuring that business processes and user access comply with legal, regulatory, and internal organizational standards.
Risk Management	The process of identifying, assessing, and mitigating risks associated with SAP user access and business processes.
SAP Fiori and GRC	The integration of SAP Fiori with SAP GRC Access Control to provide a user-friendly interface for managing access and compliance tasks.

Concept/Term	Definition
Access Certification	The process of periodically reviewing and confirming that user access rights are still appropriate for their roles, ensuring compliance.
Mitigation Control	A workaround process used when an SoD conflict cannot be eliminated directly, reducing the risk associated with the conflict.
Critical Access	Permissions in SAP that provide elevated access to sensitive functions, which require additional scrutiny and approval due to their security impact.
User Access Review	A process where user access rights are periodically reviewed by authorized personnel to ensure compliance with SoD policies.
Role-Based Access Control (RBAC)	A method of restricting system access to authorized users based on their roles within an organization, ensuring proper segregation of duties.

Concept/Term	Definition
Business Role	A role defined within SAP GRC that specifies the permissions a user requires to perform their job functions, based on business activities.
User Role Assignment	The process of assigning roles to users based on their responsibilities within the SAP system, ensuring appropriate access permissions.
Conflict Resolution	A process in SAP GRC to resolve conflicts that arise when users request access that violates SoD policies or compliance regulations.
Risk Mitigation Plan	A strategy implemented to address identified risks related to user access, including the use of compensating controls or process adjustments.
Audit Logging	A process that tracks and logs user activities within SAP to ensure transparency and accountability, supporting compliance efforts.

Concept/Term	Definition
Access Control Policy	A set of guidelines within SAP GRC that defines how user access is granted, reviewed, and maintained to protect organizational assets.
Separation of Duties (SoD) Matrix	A tool in SAP GRC used to define which duties should not be performed by the same individual, helping to prevent fraud and ensure compliance.
Access Control Dashboard	A user interface in SAP GRC that provides an overview of access risk analysis, SoD conflicts, and other relevant access control metrics.
GRC Access Control Workflow	A predefined process in SAP GRC that automates the steps involved in granting or reviewing user access, ensuring efficiency and compliance.
Emergency Access Management (EAM)	A process in SAP GRC that allows users to temporarily access critical functions or data outside of standard roles, with proper authorization and logging.

Concept/Term	Definition
Access Request Workflow	A predefined workflow in SAP GRC for processing user requests for system access, involving approval, provisioning, and access assignment steps.
Privileged User Access	Access granted to users who have elevated privileges, such as system administrators, requiring stricter controls and monitoring.
User Account Management	The process of creating, managing, and deactivating user accounts in SAP, ensuring that users only have the necessary access for their roles.
System Access Logs	Logs generated by SAP systems that record user access events, which are essential for auditing and ensuring compliance with security policies.
GRC Risk Categories	Different types of risks identified in SAP GRC, such as access risks, compliance risks, and segregation of duties risks, that need to be mitigated.

Concept/Term	Definition
Sensitive Transactions	Specific transactions or activities in SAP that involve high-risk data or processes, requiring stricter access control and monitoring.
Business Role Mapping	The process of aligning users' SAP roles with business roles to ensure they have appropriate access to perform job functions.
Access Control Ruleset	A set of rules defined in SAP GRC that governs how access is granted, reviewed, and managed, based on business requirements and compliance regulations.
GRC Access Control Dashboard	A tool that provides visualizations and analytics to monitor user access activities, potential risks, and compliance status in real-time.
Security and Compliance Reporting	The generation of reports in SAP GRC to track user access violations, SoD conflicts, and other compliance-related activities.

Concept/Term	Definition
Access Risk Analysis (ARA)	A feature within SAP GRC that identifies and analyzes access-related risks, ensuring that all users have appropriate roles and permissions.
Role Mining	A process in SAP GRC that analyzes existing user roles and permissions to identify optimal role configurations and mitigate SoD conflicts.
Segregation of Duties (SoD) Ruleset	A set of predefined rules in SAP GRC that defines the acceptable combinations of roles and permissions to ensure proper segregation of duties.
Firefighter ID	A special user ID in SAP GRC used for emergency access to systems, allowing authorized personnel to perform tasks outside normal role restrictions.
Access Control Mitigation	A process of compensating for SoD violations by implementing manual or automated controls to reduce risk in SAP GRC.

Concept/Term	Definition
Role-Based Access Assignment	The process of granting system access based on a user's role, ensuring that employees only have access to the functions necessary for their work.
Automated Access Control	A method of automating the access control process in SAP GRC, reducing manual effort and ensuring timely compliance and access reviews.
Authorization Object	A security object in SAP used to define and control access to specific functions or data based on a user's role or job function.
Segregation of Duties Analysis	The process of evaluating user roles in SAP to ensure that there are no conflicting duties that could result in fraudulent activities or errors.
Workflow Engine	A tool within SAP GRC that automates business processes like approval workflows for access requests, role assignments, and compliance reviews.

Concept/Term	Definition
Access Control Audit	The process of reviewing and auditing user access in SAP systems to ensure that it is in compliance with company policies and regulatory standards.
Access Risk Management	A set of tools and processes in SAP GRC for identifying, assessing, and mitigating risks related to user access and system security.
Temporary Access	A limited-time access granted to users for specific tasks or emergency situations, often managed and monitored by SAP GRC.
GRC Dashboard	A centralized platform in SAP GRC that provides real-time insights into access control, risk analysis, compliance, and audit results.
Role Conflict Resolution	The process of resolving conflicts in SAP GRC when a user is assigned roles that violate SoD principles, typically through mitigation or reorganization.