GLOSSARY OF SAP S/4HANA SECURITY

A Quick Reference Guide to SAP Terminologies

Get any SAP Video course -https://zarantech.teachable.com/courses/category/sap
Linkedin Learner Community page -https://www.linkedin.com/showcase/sap-learner-community/

SAP S/4HANA Security Key Concepts

Concept/Term	Definition
SAP S/4HANA Security	Practices and tools to protect data and processes in SAP S/4HANA systems.
User Authentication	Verifying the identity of users accessing SAP S/4HANA, often using usernames and passwords.
Single Sign-On (SSO)	A system that allows users to log in once and access multiple SAP applications without needing to re-enter credentials.
Role-Based Access Control (RBAC)	A security method where users are granted access based on their roles within the organization.
Authorization Objects	SAP-defined objects that determine what a user can access and perform in the system.
Security Audit Log	A log that records all actions performed by users for security monitoring and compliance.

Concept/Term	Definition
Fiori Security	The security settings for SAP Fiori apps, ensuring proper user access and data protection.
Secure Network Communications (SNC)	A protocol that encrypts data in transit between SAP systems to secure communications.
Data Encryption	The process of converting data into a coded format to protect it from unauthorized access.
User Roles	A set of permissions assigned to a user that defines what they can access and do within SAP S/4HANA.
SAP GUI Security	Configurations to secure access to SAP systems via the SAP GUI (Graphical User Interface).

Concept/Term	Definition
Password Policies	Rules that define password strength and expiration to ensure secure user authentication in SAP S/4HANA.
System Access Control	Restrictions placed on system access based on user roles and permissions, ensuring only authorized users can interact with certain features.
Identity Management	The process of managing user identities and their access rights within SAP S/4HANA.
Multi-Factor Authentication (MFA)	A security method that requires two or more forms of verification, such as password and fingerprint, to access SAP systems.
Authorization Profiles	Profiles that group together authorization objects for easy user access assignment in SAP S/4HANA.

Concept/Term	Definition
Segregation of Duties (SoD)	Ensuring that no one individual has too much control over critical tasks, reducing the risk of fraud or error.
Access Control List (ACL)	A list that defines the permissions a user or group has for accessing system resources within SAP S/4HANA.
Sensitive Data Management	Managing and protecting sensitive data (like personal or financial info) to ensure confidentiality and compliance.
Access Log Monitoring	The process of reviewing logs to track who accessed what data in SAP S/4HANA, ensuring security compliance.
System Security Patches	Updates or fixes to the SAP system that address vulnerabilities or bugs to enhance security.

Concept/Term	Definition
Encryption Key Management	The process of creating, distributing, and managing keys used to encrypt sensitive data within SAP S/4HANA.
Network Security	Protecting SAP S/4HANA communications from unauthorized access or attacks, often using firewalls and encryption.
User Permissions	Specific access rights assigned to users, indicating what they can view, edit, or delete in SAP S/4HANA.
Data Masking	The process of hiding sensitive data by replacing it with a fictitious equivalent, often used in testing environments.
Audit Trail	A chronological record of system activities used for tracking and verifying user actions in SAP S/4HANA.

Concept/Term	Definition
Risk Management	The process of identifying, assessing, and mitigating risks related to security within SAP S/4HANA.
Security Configuration	The process of setting up security controls and parameters in SAP S/4HANA to protect the system from unauthorized access.
System Integrity Checks	Procedures to ensure the security and correctness of data and system configurations within SAP S/4HANA.
Cloud Security	Security measures applied to SAP S/4HANA when hosted in the cloud to protect data and ensure compliance.
Compliance Monitoring	The process of ensuring that SAP S/4HANA security settings comply with regulatory standards and organizational policies.

Concept/Term	Definition
User Access Review	The practice of regularly reviewing and validating user access rights to ensure appropriate permissions are granted.
Role Mining	The process of analyzing user roles and behavior in SAP S/4HANA to optimize role definitions and security settings.
Critical Security Vulnerabilities	Identifying and fixing security weaknesses in SAP S/4HANA that could potentially be exploited.
Security Tokens	A form of identification used for user authentication, often used in API or system access requests within SAP.
SAP Security Patch Day	A scheduled day where SAP releases security patches and updates to fix vulnerabilities in the system.

Concept/Term	Definition
Access Request Management	The process of requesting, approving, and granting access to SAP systems and resources based on user roles.
Seamless User Authentication	The process of allowing users to transition between SAP applications without needing to re-authenticate, improving the user experience.
Role-Based Segmentation	Grouping users into roles based on their function and responsibilities to assign the appropriate level of access in SAP S/4HANA.
User Activity Monitoring	Continuous tracking of user actions within SAP S/4HANA to detect suspicious behavior and ensure compliance.
Data Access Control	Restricting access to sensitive data in SAP S/4HANA to ensure only authorized users can view or modify it.

Concept/Term	Definition
Security Audits	Regular assessments and inspections of SAP systems to check for security gaps and compliance with security policies.
SAP Security Fundamentals	Basic principles and concepts that form the foundation of security practices within the SAP S/4HANA environment.
Security Roles and Profiles	The configuration of user roles and profiles that control access to specific SAP S/4HANA applications and data.
SAP GRC	Governance, Risk, and Compliance module that integrates with SAP S/4HANA to manage security and compliance processes.
Two-Factor Authentication (2FA)	A security method requiring two forms of identification, enhancing SAP S/4HANA login security.

Concept/Term	Definition
Security Incident Response	The process of responding to and resolving security threats and breaches within SAP S/4HANA.
Firewall Configuration	The setup of a firewall to protect SAP S/4HANA systems from unauthorized network access or cyber-attacks.
Security Patch Management	The process of applying security updates and patches to SAP S/4HANA to fix vulnerabilities and enhance system protection.
SAP Security Profile	A set of security attributes assigned to a user or system, defining the specific access rights and restrictions in SAP S/4HANA.
Access Control Policy	Rules and guidelines that define how users are granted or denied access to different parts of SAP S/4HANA systems.