CONCEPT

ERP Security and Segregation of Duties: Role Design, Fraud Controls and Access Reviews

7 – 11 June 2027
London - Central London four-star



ERP Security and Segregation of Duties: Role Design, Fraud Controls and Access Reviews

Ref: 819_20253 **Date:** 7 – 11 June 2027 **Location:** London - Central London four-star **Fees:** 25300 SAR

Introduction:

ERP security and segregation of duties break down quietly: roles accumulate conflicting transaction codes, firefighter IDs stay open for weeks, vendor bank details change without a second approver and payroll ghost employees pass unnoticed through automated runs. This Core Concept course equips ERP security, audit and finance systems staff to design authorisation concepts, build SoD conflict rule sets, govern emergency access, lock down master data and spot fraud patterns inside procure-to-pay, order-to-cash and payroll. Participants produce an SoD Risk Matrix and Access Review Plan for a case ERP.

Course Objectives:

- Design a vendor-neutral ERP authorisation concept with single, composite and derived roles tied to business process ownership
- Build and tune a segregation of duties rule set that maps incompatible authorisation, custody, recording and reconciliation actions to ERP permissions
- Govern sensitive and firefighter access with ticketed requests, time-boxed IDs and reviewed activity logs
- Run user provisioning, role owner approvals and periodic user access recertification campaigns with evidence retained
- Detect fraud red flags in procure-to-pay, order-to-cash and payroll transactions using ERP tables, change documents and analytics queries
- Remediate SoD conflicts through role redesign or documented mitigating controls tracked on a remediation register

Target Audience:

- Staff who administer ERP roles, authorisation profiles and user master records
- Staff who own segregation of duties rule sets and conflict remediation for finance and supply processes
- IT auditors who examine ERP authorisations, change documents and emergency access usage
- Internal control staff who design and test mitigating controls over finance system transactions
- Finance systems analysts who maintain vendor, customer, employee and bank master data

Course Outline:

Day 1: ERP Security Architecture and the SoD Problem

- ERP Security Layers: Application Server, Database, Operating System and Client Access Paths
- Authorisation Objects, Transaction Codes, Menus and Organisational Level Fields
- Incompatible Function Model: Authorisation, Custody, Recording and Reconciliation
- SoD Conflict Anatomy: Create Vendor Plus Pay Vendor and Similar Toxic Combinations
- Current-State ERP Access Baseline: User Counts, Generic IDs and Superuser Profiles

Day 2: Role Design, Authorisation Concepts and SoD Rule Sets

- Role-Based and Attribute-Based Access Control Models for ERP Roles
- Single, Composite and Derived Role Architecture with Naming Conventions
- Business Process Risk Catalogue for Procure-to-Pay, Order-to-Cash, Record-to-Report and Hire-to-Retire
- SoD Conflict Matrix Construction: Functions, Actions, Permissions and Risk Ratings
- Rule Set Tuning: Organisational Level Filters, False Positive Removal and Critical Action Lists

Day 3: Access Lifecycle, Firefighter IDs and Master Data Controls

- User Provisioning Workflow: Request, Role Owner Approval, SoD Simulation and Assignment
- Periodic User Access Recertification Campaigns and Leaver Removal Evidence
- Firefighter and Emergency Access: Time-Boxed IDs, Reason Codes and Log Review
- Change Document and Configuration Table Logging for Client Settings and Posting Periods
- Master Data Controls for Vendor Bank Details, Customer Credit Limits and Employee Pay Records

Day 4: ERP Fraud Red Flags, Continuous Controls Monitoring and Remediation

- Procure-to-Pay Red Flags: Duplicate Invoices, Split Purchase Orders and One-Time Vendors
- Order-to-Cash Red Flags: Credit Memo Abuse, Price Overrides and Unapplied Cash
- Payroll Red Flags: Ghost Employees, Retroactive Pay Changes and Shared Bank Accounts
- Continuous Controls Monitoring Rules on Access Conflicts, Configuration Settings and Transactions
- Mitigating Control Library, Compensating Review Evidence and SoD Remediation Register

Day 5: Case ERP: SoD Risk Matrix and Access Review Plan

- Case ERP Brief: Distribution Business Role Extract and Conflict Report Analysis
- Conflict Triage Exercise: Role Redesign Versus Mitigation Decisions per User
- Firefighter Log and Vendor Master Change Report Examination for Suspicious Patterns
- SoD Risk Matrix and Quarterly Access Review Plan Assembly
- SoD Risk Matrix and Access Review Plan Defence Before a Control Owner Panel

Skills You Will Gain:

- ERP Authorisation Concept Design
- SoD Rule Set Engineering
- Emergency Access Governance
- User Access Recertification
- ERP Master Data Protection
- Transaction Fraud Pattern Detection
- Continuous Controls Monitoring Design
- Mitigating Control Documentation

Why Attend This Course:

- Take back an SoD Risk Matrix and Access Review Plan built on a case ERP and ready to adapt to your own system
- Cut the volume of false conflicts in your SoD reports so control owners act on the ones that matter
- Close the gaps that let firefighter IDs, vendor bank changes and payroll edits slip past review
- Compare ERP role design and fraud detection practice with security, audit and finance systems peers from several sectors

Conclusion:

Protecting an ERP from misuse depends on roles that separate incompatible duties, access that is reviewed and master data that cannot be changed unseen. The course moves from security layers and conflict anatomy, through role architecture and SoD rule sets, to provisioning, recertification, firefighter access and master data controls, then to fraud red flags, continuous controls monitoring and remediation. The final day applies the method to a case ERP and produces an SoD Risk Matrix and Access Review Plan.