SAP Security Concepts, Segregation of Duties, Sensitive Access & Mitigating Controls

Jonathan Levitt
March 2015
Agenda

1. Introduction
2. SAP Security Design Overview
3. The SAP Authorization Concept
4. Approaches to SAP Security
5. Segregation of Duties & Sensitive Access
6. Mitigating Controls
7. Questions
Objectives

At the end of the session, the participant will:

- Gain an understanding of the SAP security environment and why security is important to the audit;
- Define and understand what a segregation of duties conflict in SAP is, and how to monitor/address it; and
- Define and understand mitigating controls.
SAP Security Design Overview
SAP Security Design Overview

Introduction

What is SAP Security Design?

At its most fundamental level, SAP Security Design refers to the architectural structure of SAP security roles. However, effective security design is achieved via the convergence of role architecture:

1. SAP Security Organizational Structure & Governance
   - Ownership, Policies, and Accountability

2. SAP Security Processes
   - User Provisioning, Role Change Management, Emergency Access

3. Ongoing Management & Monitoring of the Security Environment
   - KPIs, Recertification, “Get Clean & Stay Clean”
SAP Security Design Overview

Introduction

Effective SAP Security Design

Org Structure & Governance

SAP Security Architecture

Security & Provisioning Processes

Monitoring

Management
SAP Security Design Overview

SAP Security Design Challenges

- User provisioning process with insufficient automation & information
- Role Change Mgmt lacks risk and quality controls
- Inefficient emergency support process

- Management KPIs for Security Design are not established
- Lack of automation for ongoing monitoring & recertification procedures
- Insufficient SoD and/or Mitigating control frameworks

- Misalignment of IT vs Business Objectives
- Lack of Strategic Security Design Decisions
- No Role or Security Design Ownership

- Overly Complex Security Design
- Lacks flexibility to respond to ongoing changes
- Lacks scalability to grow with organization
- Inefficient Role Build Approach
- No Documentation of Security Control Points
- Inherent Segregation of Duties Risk

Effective SAP Security Design
**SAP Security Design Overview**

**Audit Issues & Complexity**

- Poor security can lead to audit issues
  - When access controls are not in place, it impact the amount of reliance audit can place on reports coming from SAP
  - Segregation of Duties is a key underlying principle of internal controls, and is the concept of having more than one person required to complete a task. Security can have a detrimental impact on this control (to be discussed in greater detail later in presentation).

- It is sometimes difficult for auditors to dig deep into SAP because security is complex:
  - In SAP ERP 6.0
    - 108,000 transaction codes
    - 2,600 authorization objects
  - Several transaction codes can perform similar tasks
The SAP Authorization Concept
The SAP Authorization Concept
Introduction
The SAP Authorization Concept
Introduction (continued)

Security within the SAP application is achieved through the authorization concept.

The authorization concept is to help establish maximum security, sufficient privileges for end users to fulfil their job duties, and easy user maintenance.
The SAP Authorization Concept
Three levels of security in SAP

User master
User requires valid user-ID and password

T-code check
User requires an authorization for transactions

Authority check
User requires an authorization for underlying authorization objects and field values
The SAP Authorization Concept

The Components

**SAP User Master Record**
Master data for SAP users

**Profiles**
Container of authorizations

**Authorization Object:**
Template for security that contains fields with blank values

**Roles**
Contains transaction codes, authorizations (mapped to one profile) and user assignments

**Authority Check**
Performed by SAP to help establish that a user has the correct authorization to execute a particular task.

**Authorization (Field Values):**
Authorization object with completed fields
Let’s make an analogy... the Lock and the Key

To open the lock, the proper key must be cut specifically for a certain lock
The SAP Authorization Concept
User Types

User Type

- Dialog: A
- System: B
- Communication: C
- Service: S
- Reference: L

SAP Authorization Structure

- User
- Role
- Profile
- Authorization
The SAP Authorization Concept
Authorization Structure

Authorization is not the same as transaction. Why?

In SAP, you can perform the same function with different transactions.
The SAP Authorization Concept
Authorization Structure (continued)

SAP Authorization Structure

- User
- Role
- Profile
- Authorization
- Authorization Field Values

SAP Program Access Elements

- SAP is delivered with about 1500 authorization objects
- An object is a structure provided by SAP to grant access to a data element or a task in a specific content.
The SAP Authorization Concept
Authorization Structure (continued)

SAP Authorization Structure

Menu Items

Authorization Data

USOBT_C
USOBX_C
(SU24)

SAP Authorization Structure

User

Role

Profile

Authorization

Authorization Field Values

SAP Program Access Elements

Authorization Object

Authorization Object Fields

March 2015
The SAP Authorization Concept
Why are authorization objects required?

In SAP, you can perform the same function with different transactions:

Transaction Code

- **MK01**
- **FK01**
- **XK01**

Conventional approach protection via menu/function

SAP approach protection once via authorization

Create Vendor
The SAP Authorization Concept
The Authority Check

Transaction Code check:

<table>
<thead>
<tr>
<th>Object</th>
<th>S_TCODE</th>
<th>Start T Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field 1</td>
<td>TCD</td>
<td>FB03</td>
</tr>
</tbody>
</table>

Authorization check:

<table>
<thead>
<tr>
<th>Object</th>
<th>F_BKPF_BUK</th>
<th>Display posting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field 1</td>
<td>ACTVT</td>
<td>Display</td>
</tr>
<tr>
<td>Field 2</td>
<td>BUKRS</td>
<td>Company Code</td>
</tr>
<tr>
<td></td>
<td></td>
<td>03</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1000</td>
</tr>
</tbody>
</table>
Approaches to SAP Security
**SAP Security Approaches**
Task Based vs. Job Based Security Design

**Job Based:**
- Security is built based on positions/jobs within the organization, such as AR credit associate.
- Provisioning access is based on job responsibilities.
- Smaller number of roles per user – increased risk for granting functionality more than once.
- Transaction codes and authorizations typically duplicated in many roles.
- Users may be granted more access than necessary as a result of “additional job” or backup responsibilities.
- Appropriate for static organizations.

**Task Based:**
- Security is built based on small, definable tasks, executed by the user, such as process cash receipts.
- Larger number of roles per user – decreased risk of duplicate access.
- Transaction codes in one roles with minimal exceptions.
- User assignment flexibility – simple to grant additional access to only the tasks necessary.
- Supports future growth and sustainability – role modification decreased as a result of functionality improvements and rollouts.
- Appropriate for dynamic organizations.
SAP Security Approaches
Job Based Security Design

- Security roles are built based on positions/jobs for a group of users (e.g. Accounts Payable Clerk).
- A single role contains the access to perform a job.
- Transaction codes and authorizations typically duplicated in many roles.
A task-based design begins by bucketing transactions into one of 4 access tiers: General, Display, Functional and Control Point. Task-based roles contain access to only one of these tiers.

**TIER 1: GENERAL ACCESS**
General access is provisioned via one single role made up of tasks common to users such as printing, inbox, SU53, etc.

**TIER 2: DISPLAY ACCESS**
Display access is provisioned via a set of roles defined by functional area that allow display and reporting access intended to compliment the functional roles of the users.

**TIER 3: FUNCTIONAL ACCESS**
Functional access is provisioned via multiple single task based roles. Role grouping of activities that are the lowest common denominator of tasks and permission components to suit the needs of the end-users. These groupings usually are SoD free and part of a sub-process such as Invoice Processing or Material Master Maintenance.

**TIER 4: CONTROL POINTS**
Roles that provide additional control point access or granularity needed by Tiers 1-3 such as Company Code, Plant, etc.
SAP Security Approaches
Task Based Security Design (continued)

- Security roles are built based on positions/jobs for a group of users (e.g. Accounts Payable Clerk).
- User assigned to the tasks needed to perform his/her job (not a job-based role)
- User receives multiple single roles
- Flexibility to each individual user’s role assignments
Segregation of Duties & Sensitive Access
**Segregation of Duties & Sensitive Access**

**Introduction**

**Segregation of Duties**

A segregation of duties risk is when a combination of abilities that when assigned to a backend user constitutes a risk.

Objective of this risk is to facilitate the appropriate division of responsibilities.

**Sensitive or Critical Access**

A sensitive or critical access risk is where the direct assignment of an ability to a backend user constitutes a risk.

Objective of this risk is to help establish that access is restricted to the appropriate individuals.
**Segregation of Duties & Sensitive Access**

**Introduction (continued)**

### Segregation of Duties

Example risk:

*Maintain Accounting Periods vs. Post Accounting Document in GL*

Allow a user to inappropriately open accounting periods previously closed and fraudulently post documents to that period after month end.

### Sensitive or Critical Access

Example risk:

*Post Accounting Document in GL*

Should be restricted to authorized users to thereby decrease the risk of fraudulent, malicious or erroneous journal entries being posted.
Segregation of Duties & Sensitive Access
Examples

- **Finance:** Maintenance of accounting periods should be segregated from the posting of financial transactions in the wrong period.

- **Inventory:** The receipt/maintenance of inventory should be segregated from order and invoicing activities.

- **Accounts Payable:** Reconciling and releasing blocked vendor invoices should be segregated from daily processing and posting activities.

- **Procurement:** Maintenance of contracts and terms should be segregated from payment and billing document changes.
Segregation of Duties Walkthrough
Segregation of Duties Walkthrough

Business SOD/SA Rule

Ability Level

Ability 1
Create PO

Ability 2
Release PO

and

Function Level

Function (TCode) ME21N or Function (TCode) ME25 or Function (TCode) ME27 or Function (TCode) ME29N or Function (TCode) ME28

and

Object Level

Object 1 M_BEST_BSA and Object 2 M_BEST_EKG and Object 3 M_BEST_EKO

and

Field Value Level

Field 1 EKORG 100 or 200 and Field 2 ACTVT 01 – create
Segregation of Duties & Sensitive Access
How to monitor?

- Companies have many different ways to monitor segregation of duties and sensitive access:
  - SAP GRC Access Control
  - Other access control systems (Approva, ControlPannel, SecurityWeaver, ACL, etc.) or “homegrown” monitoring tools
  - Reporting transaction code “SUIM”.

March 2015
Mitigating Controls
**Mitigating Controls**

Introduction

**Defining and applying Mitigating Controls**

If violating access cannot be remediated as there is a legitimate business purpose for access then mitigation is going to be required. Mitigating controls are designed to cover the residual risk of a user having that access.

For example, if a business unit is too small to segregate duties in the purchasing department and users must have the ability to create and approve purchase orders for the business to function, the business may choose to establish a mitigating control to analyze transactions by users with access to both sides of the SOD conflict to mitigate the risk:

- **Risk:** A user can create and approve a fictitious PO.
- **Key Control:** The ability to release (approve) and create purchase orders is segregated.
- **Mitigating Control:** Location supervisor analyze purchase orders entered into SAP by the two Purchasing Clerks from the business unit.
Mitigating Controls
Considerations

Is the risk truly a risk for compliance requirement?

No

Deactivate or Switch to Low Risk

Yes

Determine the controls in place that mitigate

Scenario 4: Detective Controls
Management has detective controls in place that mitigate the associated risk.
Management does not intend to segregate the access in the system to mitigate the risk in a preventive manner.

Scenario 3: Remediation of Access Occurring
Management intends to enforce the SOD however most users currently have access as the business processes require redesign and/or the access remediation.
Detective controls (mitigating) are put in place while remediation occurs.

Scenario 2: Some Users Require Access
The SOD is enforced partially in the environment, most users do not have the access, however some need it.
Detective controls (mitigating) are put in place for these users.

Scenario 1: No intent to grant access.
Management does not intend that any users receive access to the risk. No mitigating controls should be created.

Preventive

Detective

Mitigation Process

March 2015
Questions?