Case Study of a Segregation of Duties Project

Applies to:

SAP Security, SAP GRC Access Control Suite
For more information, visit the Security homepage.

Summary

As Companies today are struggling to meet the Compliancy and regulatory requirements of their SAP Systems, Segregation of Duties plays a key role in the SAP Security design and implementation. Segregation of Duties means that no single user will have the authorizations to all key steps in a business process. This article will explain some of the important details that need to be understood while implementing the SoD project in a typical SAP landscape.

Author: Kiran Kandepalli

Company: Intelligroup Inc

Created on: 13 October 2008

Author Bio

Kiran Kandepalli is working with Intelligroup Inc as a Principal Consultant in SAP Security/SAP GRC related projects in USA.

© 2008 SAP AG

Table of Contents

1. Introduction 3
2. Segregation of Duties Concept 3
2.1 Incompatible Job Functions 3
2.2 What is an SOD Risk? 4
3. Implementation Details of an SoD Project 4
3.1 Creation of an SoD rule set 4
3.1.1 Functions 4
3.1.2 SoD Conflicts 5
3.1.3 Critical Transactions 5
3.1.4 Critical Authorizations 5
3.1.5 Critical Roles 5
3.1.6 Critical Profiles 5
3.2 SoD Conflict Analysis 5
3.2.1 Role Level Analysis 6
3.2.2 User Level Analysis 6
3.3 Remediaton of SoD Conflicts 6
3.4 Mitigation of SoD Conflicts 6
3.5 Segregation of Duties for Background Users 7
Related Content 8
Disclaimer and Liability Notice 9

© 2008 SAP AG

1. Introduction

Segregation of Duties (SoD) has become an important prerequisite in the implementation of every compliance related project all over the world. As the name suggests that no single user can have access to all authorizations of a process end to end. It is required that job duties in each business process are completely segregated and adequate controls need to be placed. The role of a SAP Security consultant is vital in the design of SAP Security Roles and Authorizations and appropriate SoD remediation and Mitigation Controls are put in place.

2. Segregation of Duties Concept

The underlying concept of Segregation of Duties is that no one person should have excessive control over one or more critical business processes.

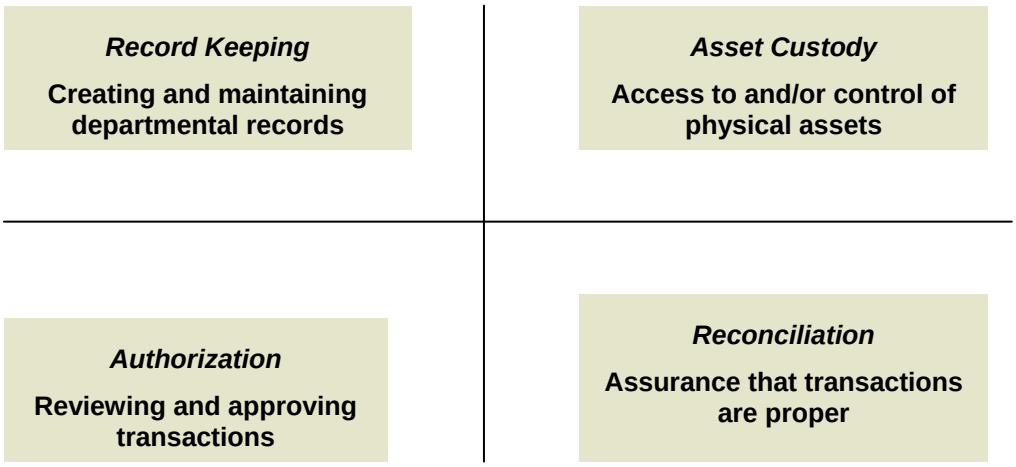
When dealing with Access controls for example, a person should not be able to grant himself/herself rights and then perform the action. Similarly, they should not be able to perform a transaction and then delete all the logs that tracked the activity. Instead, processes should be properly reviewed and separated in order to reduce the risks associated with a process being compromised either maliciously or through human error.

Understanding and applying SOD controls are vital to information security.

Segregation of duties issues come up frequently in security reviews and audits. Rather than being viewed as arcane control concepts, SOD controls should be recognized as additional means to help manage risks. Like all controls, there will be limits to what organizations can do. To help address concerns, a review can be undertaken to properly align roles with business needs while properly addressing the risks associated with improper segregation of duties.

2.1 Incompatible Job Functions

To maintain proper Segregation of Duties, no employee should be responsible for two or more of the following four functions for a single transaction class:



© 2008 SAP AG

2.2 What is an SOD Risk?

- Segregation-of-Duties risks are opportunities for one individual to control a process from beginning to end without the involvement of others.
- When an individual exploits the condition, data integrity, productivity loss, and physical losses can result without being detected.
- For example, one person may be able to set up a vendor and process payments

  SOD RISK – Access to both FB60 (Enter Vendor Invoice) and F-07 (Post Payments) transactions

3. Implementation Details of an SoD Project

The following activities are performed during the implementation of SoD Project.

3.1 Creation of an SoD rule set

Every company needs to follow compliancy procedures and regulations in accordance with SOX act and FDA rules. There will be a set of predefined Process Control and Access Control rule sets that come with the SoD tool like SAP GRC that can be used. Company Internal Auditors and SoD team will identify Custom rule sets if needed. The following entities comprise a SoD Rule set.

3.1.1 Functions

A common group of SAP Transaction codes and Authorization objects that fulfill a particular Business Process is termed as a “Function”. Each of these Functions is very critical for the Business. Create a four character Function ID for each of the Critical Business Processes.

For example: The function ***Process Goods Receipt (PO01)*** contains the following common transactions:

MB01 *Post Goods Receipt for PO*

MB02 *Change Material Document*

MB0A *Post GR for PO*

MB1C *Other Goods Receipt*

MB31 *Goods Receipt for Production Order*

MIGO *Goods Movement*

MIGO_TR *Transfer Posting*

COGI *Process Goods Movement w. Errors*

The function ***Create and Maintain Purchase Order (PO02)*** contains the following Common transactions

ME21 *Create Purchase Order*

ME22 *Change Purchase Order*

ME25 *Create PO with Source Determination*

ME27 *Create Stock Transport Order*

ME59 Automatic Generation of PO

© 2008 SAP AG

3.1.2 SoD Conflicts

When two or more critical business functions are combined then it is identified as an SoD Conflict.

Create a four character SoD Conflict ID for each of the conflicting business processes.

For example: When the above two functions Process Goods receipts (PO01) and Create and Maintain Purchase Orders (PO02) are combined and assigned to a single user, it becomes an SoD Conflict.

For example: The ***SoD Conflict P001 = PO01 + PO02***

3.1.3 Critical Transactions

All the important transactions that are critical to each business process need to be listed and documented. Access to these critical transactions is given only with appropriate approval mechanism. Whenever these transactions are executed by the users they can be logged and proper audit trail is maintained.

For example: SE38, SA38, SE16

3.1.4 Critical Authorizations

All specific sensitive authorization objects need to be listed and documented. These need to be monitored and logged too.

For example: S_TABU_DIS, S_TABU_CLI

3.1.5 Critical Roles

All the Critical Roles which are considered sensitive must be listed and documented. Whenever there is a request for access to these critical roles, it needs to be documented for Audit purposes.

For example: A Role with ABAP Debug Authorizations.

3.1.6 Critical Profiles

All the Critical Profiles that are deemed sensitive must be listed and documented.

For example: SAP_ALL, SAP_NEW.

3.2 SoD Conflict Analysis

This is a very important step in the SoD Project. The SoD Conflict Analysis must be conducted in a two step iterative approach on all the Roles and Users existing in the SAP System.

If there is an SoD tool like SAP GRC already in place then the results will be much quicker and the job can be scheduled on a daily basis to perform SoD analysis on all new roles and users.

Manual identification of SoD conflicts is often very time consuming.

© 2008 SAP AG

3.2.1 Role Level Analysis

All the Security roles comprising of Single, Derived, Composite Roles need to be checked for any Inherent SoD Conflicts. If the Roles contain any conflicting transactions and authorization objects, then those roles need to be documented for further action.

3.2.2 User Level Analysis

All the Dialog and Non-Dialog users need to be checked for any SoD Conflicts due to the assignment of any Conflicting Roles and Critical Profiles. These Users need to be documented for any further action.

3.3 Remediaton of SoD Conflicts

After the analysis of the SoD conflicts are performed at both the Role level and User level, it is very effective to do the remediation of SoD Conflicts at the Role level first as it will remove the Conflicts of all Users that are assigned to each of these roles.

For example: If one conflict is removed from a single role that is assigned to 25 users then, almost all of the 25 conflicts are gone.

Even after performing the remediation of SoD Conflicts at the Role level, there will be SoD Conflicts at User level. Each of those conflicts need to be analyzed properly and discussed with the appropriate Business Process Owners and User Managers for every action of remediation.

Any modification of Roles and authorizations as a result of this process need to be done in Development system and the modified roles and profiles need to be transported to QA for testing and after all successful testing they need to be transported into Production system.

It is advisable that the testing has to be perfomed by the End Users themselves in QA and not by the Basis/Security team so that all the Authorizations are tested well.

3.4 Mitigation of SoD Conflicts

There are times where the Business requires that the User have roles that contain functions that are conflicting in nature. If there is no way to remediate the SoD Conflicts for that particular user as business demands the authorizations to be in place, Mitigation of SoD Conflicts is only alternative. Any Mitigation Control needs to be documented and appropriate approval needs to be taken from that particular Business Process Owner before granting the authorizations to the Users.

The Mitigation Control is identified with a four character ID.

For example: If the Business demands due to lack of Buyers that a particular user be given authorization to create a Purchase Order and then Approve the Purchase Orders upto $25000, then a ***Mitigating Control M001*** is placed on that User.

© 2008 SAP AG

3.5 Segregation of Duties for Background Users

It is often debated whether the SoD Conflicts need to be applied to Background Users. But the fact is that the whole SAP system needs to be compliant including all Dialog and Non – Dialog Users. It becomes very difficult and stands as a challenge to the IT team members when asked to follow compliancy standards, rules and regulations for Non-Dialog users like Background Users. The following steps need to be taken to ensure that the Background users are free of any SoD Conflicts.

- Critical SAP Profiles like SAP_ALL and SAP_NEW must be deleted from the Background user ids and it will minus most of the SoD Conflicts.
- All the business jobs that will be run under this background id must be documented.
- New Security Role must be created and authorizations must be tailored to suit the requirements of the background jobs run by the Background user id.
- If complete remediation of SoD Conflicts is not possible, as sometimes is the case, then appropriate Mitigation Controls need to be framed and documented.

© 2008 SAP AG

Related Content

www.sdn.sap.com

help.sap.com

www.sapsecurityonline.com

www.service.sap.com

For more information, visit the Security homepage.

© 2008 SAP AG

Disclaimer and Liability Notice

This document may discuss sample coding or other information that does not include SAP official interfaces and therefore is not supported by SAP. Changes made based on this information are not supported and can be overwritten during an upgrade.

SAP will not be held liable for any damages caused by using or misusing the information, code or methods suggested in this document, and anyone using these methods does so at his/her own risk.

SAP offers no guarantees and assumes no responsibility or liability of any type with respect to the content of this technical article or code sample, including any liability resulting from incompatibility between the content within this document and the materials and services offered by SAP. You agree that you will not hold, or seek to hold, SAP responsible or liable with respect to the content of this document.

© 2008 SAP AG