Segregation of Duties – SoD

Applies to:

Segregation of Duties GRC SAP Access Control Suite.

Summary

Under growing pressure of various regulatory standards by different governments such as SOX, an US accounting law, it is clear that there should be properly defined and implemented access controls. SoD or Segregation of Duties says that an individual should not have access rights to a function/process end-to-end. There needs to be a well defined Strategy for doing Segregation of Duties effectively in an Organization that is spread across various systems and various Geographies.

Author: Nuzhat Khan

Company: HCL Technologies

Created on: 19 Oct 2007

Author Bio

Nuzhat Khan is an Associate Consultant working with HCL Technologies

Table of Contents

Segregation of Duties

Under growing pressure of various regulatory standards and measures issued by different government, it is clear that there should be properly defined access controls and implemented effectively. Access Control, ensures that there is proper segregation of duties. SoD or Segregation of Duties is an important factor while dealing with different responsibilities and job profiles across an enterprise.

Across an enterprise there are various functions and these functions are performed, together by a set of roles/responsibilities. SoD says that these set of Roles/responsibilities should be assigned in such a way that, across an enterprise, any individual should not have end to end access rights over any function. The Roles and Responsibilities for the function should be divided in such a way that one person does not full right over the function that the risk of malicious activity of manipulation of the function is reduced. The more critical the function is, greater and clearer Segregation of Duties should be.

Segregation of Duties deals with access controls. Access Control ensures that one individual should not have access to two or more than two incompatible duties. Some examples of incompatible duties are:

- Creating vendor and initiate payment to him.
- Creating invoices and modifying them.
- Processing inventory, and posting payment.
- Receiving Checks and writing pay-offs.

Ideally, single individual must not have authority of creation, modification, reviewing and deletion for any transaction / tasks / resources.

If any individual has access rights to creation and modification, he can create and after getting it reviewed, he can modify it to do some fraudulent exercises. Similarly if an individual has creation and deletion rights he can create, initiate payment and later delete any transaction logs that can track his activity.

Segregation of Duties ensures that:

- There are no errors, as SoD ensures cross check of roles/responsibilities.
- Risk of Fraud is reduced as fraud will involve two or more than two individuals.
- Clear separation of Roles/Responsibilities across various functions in organization.

Segregation of Duties must be so performed that it reduces the risk associated with a function/process that can be mal-functioned to practice any fraudulent exercises. If proper SoD does not exist in an organization, then:

- There are ineffective internal access controls.
- There is improper use of materials, money, financial assets and resources.
- Estimation of financial condition may be wrong.
- Financial documents produced for audits and review may be incorrect.

There are circumstances where proper Segregation of Duties cannot be implemented. In such cases there should be a mitigating control designed in order to keep a check on the unresolved SoD. For Example, if in case it is necessary, under some circumstances that an individual must have creation and modification rights then there should be a mitigating control designed to keep a track over the individual's activities. For example, there could be a mitigating control that could keep a check on database that is where his creation and modification transactional data is saved, or may be a review of transactional logs can be a mitigating control.

Segregation of Duties and Role Matrix

Segregation of Duties can be represented over a role matrix. Role Matrix is a two dimensional matrix. All the roles/responsibilities and functions/processes in an enterprise are recognized and they are represented over each axis of matrix. Then it is identified by putting a flag, across each set of roles/responsibilities and function/processes, over x and y – axis, whether they are conflicting or not.

Here is a sample role matrix. This role matrix has been identified for a set six processes and a set of six responsibilities, one for each process.

Roles / Function/ Processes	Create Vendor	Change Vendor	Post Goods Receipt	Post Payment	Process Inventory	Goods Issue	Maintain PO
Create Vendor		X	X	X			X
Change Vendor	X		X	X			X
Post Goods Receipt	X	X		X	X	X	X
Post Payment	X	X	X			X	X
Process Inventory			X				X
Goods Issue			X	X			
Maintain PO	X	X	X	X	X		

X - Existence of Conflict

SoD and SOX Compliance

SOX is an US Accounting law that deals with the financial accounting of the companies. In order to comply with SOX requirements, it is required that there should be well documented IT Processes. Over each of the IT Processes there should be well designed and documented internal controls and these controls should be well implemented and tracked and monitored. There should be effective controls over the key security and financial processes.

The SOX IT audit tries to identify that there are processes and controls in place and are being followed and tracked. In case of large and geographical organizations, it is not adequate for manual or paper-based processes and controls to be sufficient. There needs to be a proof that these processes are well followed and tracked.

In order to comply with section 404 of SOX, we should:

- Identify and document processes and SoD controls across key IT Security and financial processes.
- Design mitigating controls and document then, where appropriate SoD cannot be implemented.
- Design monitoring controls for critical processes and critical roles.
- Implement SoD and mitigating controls.
- Ensure continuous compliance by monitoring and tracking of controls.

SoD Implementation

For implementing SoD Controls across an enterprise, we need to do a heavy exercise. Therefore implementation SoD is done in form of a project. The implementation can be done by outlining the following steps as described below:

- Identify what is the objective of organization, hierarchy and nature of Organization, and job profiles in the organization, by doing an Organization scan.
- Identify the processes that are being followed in organization.
- Identify the current state of roles/responsibilities and authorization in the enterprise.
- Create the Role Matrix. Mark roles on one axis of Matrix and functions on other axis. Identify will there be any SoD conflict if role access to particular function is given to a single individual. Yes or No, flag the position in matrix accordingly, clearly.
- After analyzing the SoD conflict from role matrix, discuss with management and make the required changes in order to resolve SoD conflicts.
- In role matrix at position where SoD Conflicts cannot be resolved, design the mitigating controls.
- According to findings in role matrix, generate the roles and mitigating controls within the enterprise system.
- Create a document that will well-define the changes required in a simple and organized manner.
- Document various roles, processes and mitigating controls for auditing and reporting.
- Inform and report the changes required to management and as well as to those affected, to make sure changes are implemented in well organized and smooth manner.

SoD is critical in helping managing risks. SoD issues and controls come up frequently when there are audits and reviews. SoD controls can be use as step to measure and resolve the risks associated with the different roles and access to functions. To resolve the conflicts, we can design roles as per the business needs of various function/processes being executed in an enterprise.

Related Content

Following web sites were referenced:

- http://web.utah.edu
- http://en.wikipedia.org/wiki
- http://itmanagement.earthweb.com/columns
- http://www.oversightsystems.com
- https://www.sdn.sap.com

Note: For more info on the Access Control Risk management have a look at the link:

https://www.sdn.sap.com/irj/sdn/go/portal/prtroot/docs/library/uuid/0043a8ab-bdae-2910-d8bc-cf4abd4d6bed

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.