Security SOD Overview

Kailash Joshi
Associate Consultant

Agenda

1. **Introduction**
   - 1.1. Sarbanes-Oxley
   - 1.2. SoD Overview
   - 1.3. Common Issues
   - 1.4. Key Benefit of SoD
2. **SOD Management Process Phases**
3. **Methodology**
   - 2.1. Implementation of SoD
   - 2.2. Roles and Responsibilities
   - 2.3. SoD Ownership and Governance
   - 2.4. SoD Matrix Template
4. **Sod Scope: Recommendation**

Introduction

Sarbanes-Oxley has become the ad hoc standard for financial transparency, trust, and corporate accountability. While mandatory for all publicly-owned companies, Sarbanes-Oxley is also becoming a best practice for all types of companies who wish to identify with good governance practices.
A significant amount of attention is currently focused on Section 302 (Disclosure) and Section 404 (Internal Controls). Sarbanes-Oxley Sections 302 and 404 are designed to ensure information required to be disclosed is initiated, processed, recorded, and reported, and that management has assessed the effectiveness of internal controls regarding the reliability of financial reporting.

SOX Compliance

In order to comply with section 404 of SOX, following should be achieved:

•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 Overview

Segregation of duties is used to ensure that errors or irregularities are prevented or detected on a timely basis by employees in the normal course of business

Segregation of duties:

- A deliberate fraud is more difficult because it requires collusion of two or more persons, and
- It is much more likely that innocent errors will be found. At the most basic level, it means that no single individual should have control over two or more phases of a transaction or operation. Management should assign responsibilities to ensure a crosscheck of duties.

Some conflicting 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.

Common Issues

Some of the Common Issues are as follows:

- Scope and purpose is not clearly defined
- Key stakeholders are not involved
- Mitigating Controls not tested
- Risk Acceptance documentation not properly maintained
- Lack of Appropriate tools or skills. This leads to manual tracking and reporting is too labor intensive
- Ownership is not clearly defined
- Lack of Integration through the Blueprint and Relization Phase
- Global Rulesets are applied differently in local geographies
- 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.

Key Benefit

Reduced Audit & Compliance Costs

Reduced Burden on IT Staff

Certify that they have established and are maintaining internal controls

Ensure the effectiveness of such internal controls every quarter.

Address significant changes in internal controls or other factors that could significantly affect such controls.

Identify corrective actions taken regarding deficiencies/weaknesses in controls.

Disclose any significant deficiencies in internal controls and/or any fraud involving persons with a significant role in upholding such controls

Efficient and Faster compliance management – Set up most comprehensive library of SoD rules, to go live quickly and achieve a cost-effective cleanup of initial controls.

SOD Management Process Phases

Phase	Steps	Reference Documents / Tools	Objectives
Risk Recognition	Identify risk to be monitored & classify its severity	SOD Summary	Identify the threat and business effect
Rule Building and Validation	Identify the transactions and authorizations necessary for the threat.Build Transaction Code (T-Code) and SOD object rules to discover the threat.Verify rules against known cases or create test cases.	Delivered assumptions and Rule Architect in GRC Access Control	Build and customize business rules to specification to discover the threat conditions in roles and/or user assignments
Analysis	Run Analytical Reports Size exceptions Confirm rules are working Modify rules, if necessary Run Management reports.Analyze roles and users after roles are changed.	GRC Access Control Management View/Risk Analysis reports – system scans Role reports User reports	Identify role changes and/or user assignments to resolve issues.
Remediation	Determine alternatives to eliminate issues in roles.Present analysis to respective BPOs. Document corrective actionsModify/create roles or user assignments. Document mitigating controls and monitor.	Firefighter ID's to take on infrequent functions like closing periods in conflicts.Use of Risk analysis and Management View reports and Remediation analysis.Simulation for exclusions and composite utility report.	Get approval for role modifications to avoid risks inherent in roles & composites.Get approval for user changes to avoid risks. Determine conditions which cannot be corrected by role or user assignment changes.SOD issues.
Mitigation	Design alternative controls to mitigate the risk.Educate Management and get approval.Document mitigating controls and monitor.	Association of risks and corresponding access controls.Alerts for mitigating controls.	Document controls and personnel responsible for monitoring the risks and assigning alternative controls to user and role
Continuous Compliance	Complete simulation to monitor changes when requests are made for new roles, user assignments or changes.	Simulation capabilities in GRC Access Control	Maintain Continuous Controls Compliance and identify new risks on a proactive basis.

SOD Implementation Methodology

For implementing SoD Controls across an enterprise following steps can be Outlined

•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.

SoD Implementation Methodology -Contd.

•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.

Roles and Responsibilities

During SoD Implementation following Roles and Responsibilities can be defined:

Business Process Owners (BPOs) - staff responsible for protecting the integrity the information and processes supported by an IT system. BPOs are in charge of

Identifying risk and/or approving controls for monitoring risks

Approving remediation to address user access issues in the IT system

Designing alternative controls to mitigate Segregation-of-Duties issues

Communicating access assignments or role changes

Senior executives - approve or reject risks between business areas and approve mitigating controls for risks.

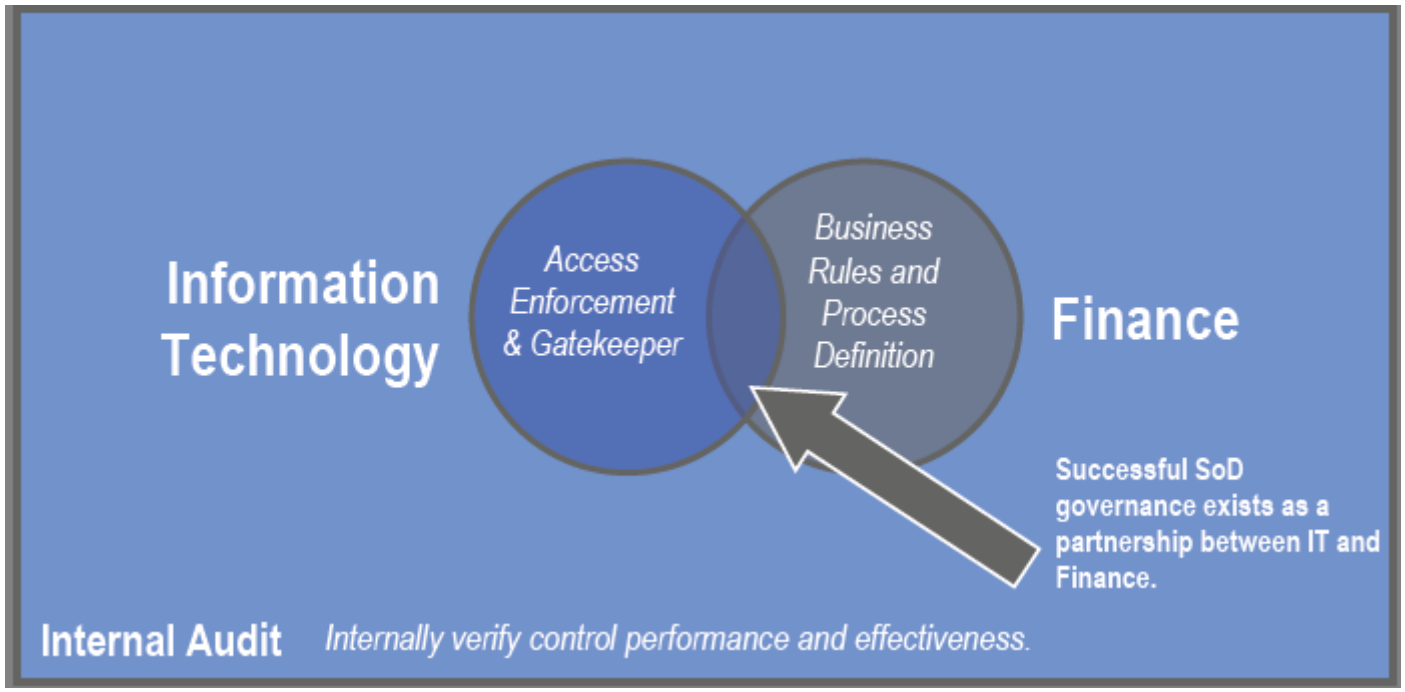
SAP security - owners of the SOD management process and associated software products who facilitate decision making as well as alternative methods to manage SOD risks.

Business Process Analysts (BPAs) - help security administrators define the technical rules for each business area for approved risk conditions and recommend alternatives to eliminate SOD risks in roles and user assignments.

Internal audit - perform risk assessments on a regular basis to identify new risks, perform periodic testing of rules and mitigating controls; act as a liaison with external auditors.

SOD rule keeper - maintains the rules in the development environment, promotes to the production environment for risk monitoring and is responsible for enforcing the process for building and gaining approval for the rules to be used.

SoD Ownership and Governance



SoD Matrix Template

Task Group Description	Grp	1 AP Voucher Entry	2 AP Payments	3 AP Release Blocked Inv	4 AP Clear Vendor Acct.	5 Vendor Mast. Maint. FI	6 Vendor Mast. Maint. MM	7 Vendor Mast. Maint. CEN	8 Bank Reconciliation	9 AR Cash Application	10 AR Clear Customer Acct.	11 Material Master Maint.	12 Service Master Maint.	13 Requisitioning	14 Release Requisition	14A Process Requisition	15 Purchase Order Entry	16 Purchasing Agreements	17 Goods Receipt on PO	18 Service Receipts Entry	19 Physical Inventory	20 Sales Agrmts/Contracts	21 Customer Master Maint.	22 Customer Master (Credit)	23 Sales Invoicing	24 Sales Invoice Release	25 Sales Order Entry	26 Sales Order Release	27 Sales Pricing Maint.	28 Sales Rebates	29 Maintain Security
AP Voucher Entry	1		HX	X	X	MX	MX	MX									X	X	HX	HX											HX
AP Payments	2	HX				HX	HX	HX	HX								HX	X													HX
AP Release Blocked Inv	3	X															X	X	X	X											HX
AP Clear Vendor Acct.	4	X															X														HX
Vendor Mast. Maint. FI	5	MX	HX				X										HX	X													HX
Vendor Mast. Maint. MM	6	MX	HX			X											HX	X													HX
Vendor Mast. Maint. CEN	7	MX	HX														HX	X													HX
Bank Reconciliation	8		HX							HX																					HX
AR Cash Application	9								HX													X	MX	MX	MX		X			X	HX
AR Clear Customer Acct.	10																					X			MX		X			X	HX
Material Master Maint.	11													X			X	X													HX
Service Master Maint.	12													X			X	X													HX
Requisitioning	13											X	X		X		X	X													HX
Release Requisition	14													X			HX	X													HX
Process Requisition	14A													X			HX	X													HX
Purchase Order Entry	15	X	HX	X	X	HX	HX	HX				X	X	X	HX				HX	HX											HX
Purchasing Agreements	16	X	X	X		X	X	X				X	X	X	X				X	X											HX
Goods Receipt on PO	17	HX		X													X	HX			X										HX
Service Receipts Entry	18	HX		X													HX	HX													HX
Physical Inventory	19																		X												HX
Sales Agrmts/Contracts	20									X	X												X	X							HX
Customer Master Maint.	21									MX												X					MX				HX
Customer Master (Credit)	22									MX												X					X				HX
Sales Invoicing	23									MX	MX															X			HX		HX
Sales Invoice Release	24																								X						HX
Sales Order Entry	25									X	X												MX	X				X	HX	X	HX
Sales Order Release	26																										X				HX
Sales Pricing Maint.	27																										HX				HX
Sales Rebates	28									X	Y																X				HX
Maintain Security	29	HX	HX	HX	HX	HX	HX	HX	HX	HX	12:35:13 PM 5/27/2009 (					HX	HX	HX	HX	HX	HX	HX	HX	HX	HX	HX	HX	HX	HX	HX	HX	

X Segregation of Duties Conflict

H High financial risk

M Medium financial risk

General Areas of Conflict

General areas of conflict that must be addressed in order to maintain effective internal controls over the business process :-

Maintenance of general accounting periods, charts of accounts, and other general infrastructure changes must be segregated from posting, changing, and adjusting capabilities for financial transactions.

Master data should be segregated from business transactions and vendor/supplier additions and maintenance should be segregated from financial transactions.

The receipt and maintenance of inventory goods or services must be segregated from order and invoicing activities.

Banking transactions and changes must be segregated from payment, vendor and posting activities.

General Areas of Conflict - Contd.

Reconciling and releasing transactions in a suspense or “blocked” status must be segregated from daily processing and posting activities.

Order, invoice and payment activities should be segregated or monitored if given to one person.

Invoice posting must be segregated from goods receipt and payment processing.

Inventory verification or pricing adjustments should be segregated from counting and stock picking activities.

Maintenance of contracts and terms must be segregated from payment and billing document changes.

Sod Scope: Recommendation

Clearly define your scope
IT Dept. is an enabler or facilitator, not owner
Internal Audit can be an owner or facilitator
Business Owners/Finance own Sod as they accept any residual risk

Invlove External Audit in your scoping exercise

Document and test mitigating controls

Document the acceptance of unmitigated risk

Preventative Controls – Proactive methods used to prevent the occurrence of the risk. For example: Separating duties between organizations and people so two people have to be involved for the fraud to occur. Another example is the regular backup of data to be able to restore critical data when destroyed.
Detective Controls – Methods used to detect the occurrence of bad events after-the-fact. For example: Reviewing key transactions completed by an individual who has the access to set up a vendor and process payments. Another example would be logging changes and reviewing for unusual or unauthorized changes.

Thank you!

Copyright 2008 SAP AG
All rights reserved