Effective Segregation of Duties (SOD) in ERPs

Steve Shofner, Senior Manager, Armanino
Junior DeAlba, Senior, Armanino

Core Competencies – C23

ISACA®
Trust in, and value from, information systems
San Francisco Chapter
2014 Fall Conference - "Think Big"
CRISC
CGEIT
CISM
CISA

Learning Objectives

- Understand what is SOD (Segregation Of Duties)?
- Understand the role SODs within ERPs (Enterprise Resource Planning) applications.
- Discuss approaches to security and segregation of duties analysis
- Understand different audit options / techniques
- Q & A

What is SOD?

What is SOD?

The Institute of Internal Auditors defines Segregation of Duties says:

“A fundamental element of internal control is the segregation of certain key duties. The basic idea underlying SOD is that no em-ployee or group of employees should be in a position both to perpetrate and to conceal errors or fraud in the normal course of their duties. In general, the principal incompatible duties to be segre-gated are:

- Custody of assets.
- Authorization or approval of related trans-actions affecting those assets.
- Recording or reporting of related transac-tions.

Traditional systems of internal control rely on assigning certain responsibilities to different individuals or segregating incompatible functions. The general premise of SOD is to prevent one person from having both access to assets and responsibility for maintaining the accountability of those assets.”

https://iaonline.theiia.org/simplifying-segregation-of-duties

What is SOD?(Cont.)

What must be segregated? The four main components:

Record Keeping

The process of creating and maintaining records of revenues, expenditures, inventories, and personnel transactions.

Custody of Assets

Having access to or control over any physical asset such as cash, checks, equipment, supplies, or materials.

Authorization

The process of reviewing and approving transactions.

Reconciliation

Verifying the processing or recording of transactions to ensure that all transactions are valid, properly authorized, and properly recorded on a timely basis.

Understanding SOD’s Role

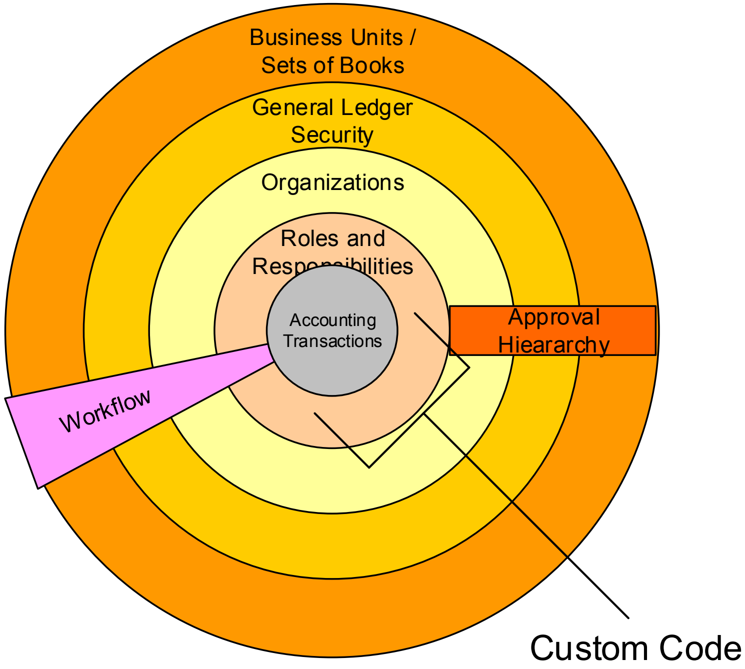
What is SOD?(Cont.)

Why Segregate Duties?

Key factor that for the existence of Segregation of Duties to provide assurance that transactions are:

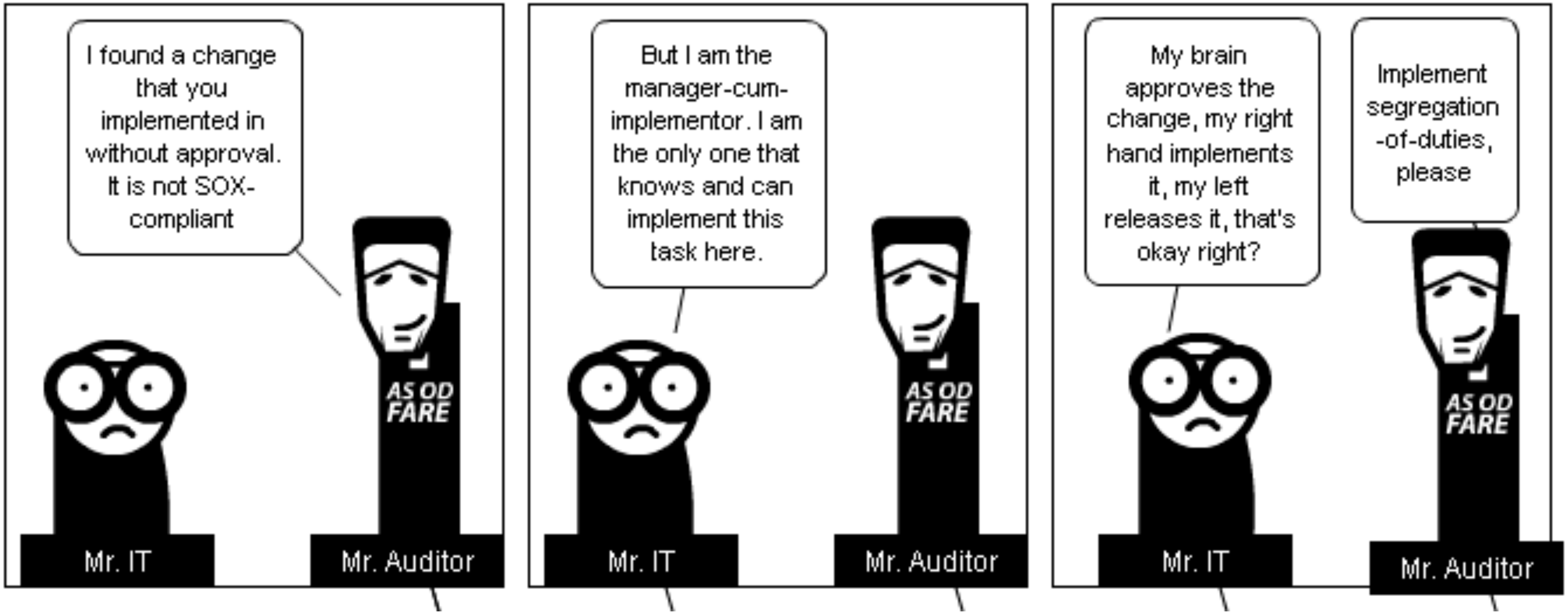
- ✓Valid
- ✓Reported Accurately
- ✓Comply with rules and regulations
- ✓In accordance with organizations objectives

Segregation of Duties in ERP



Segregation of Duties in ERP applications can be a multi-dimensional challenge. ERP application security should be understood from the different layers to assess the full nature of segregation of duties weaknesses.

Audit Humor (**EVERYONE LAUGH!**)


I found a change that you implemented in without approval. It is not SOX-compliant
Mr. IT
AS OD FARE
Mr. Auditor
But I am the manager-cum-implementor. I am the only one that knows and can implement this task here.
Mr. IT
AS OD FARE
Mr. Auditor
My brain approves the change, my right hand implements it, my left releases it, that's okay right?
Implement segregation-of-duties, please
Mr. IT
AS OD FARE
Mr. Auditor

Evaluating Your SOD

Types of risks in ERP's caused by SOD issues

- **Excess Access**- a user having two or more business processes that could result in compromise of the integrity of the process, data or allow that person to commit fraud
- **Access to sensitive functions** – a user having access to a function that, in and of itself, has risk
- **Access to sensitive data** – a user having access to sensitive data such as employee identification number (US= SSN), home addresses, credit card, bank account information, plus data unique to an organization– customers, BOMs, routings…

An Approach to Evaluating SOD

- Create a Policy
- Identify the core tasks performed at your company
- Identify incompatibilities
- Create / Edit user roles to remove conflicts
- Test revisions
- Deploy revisions

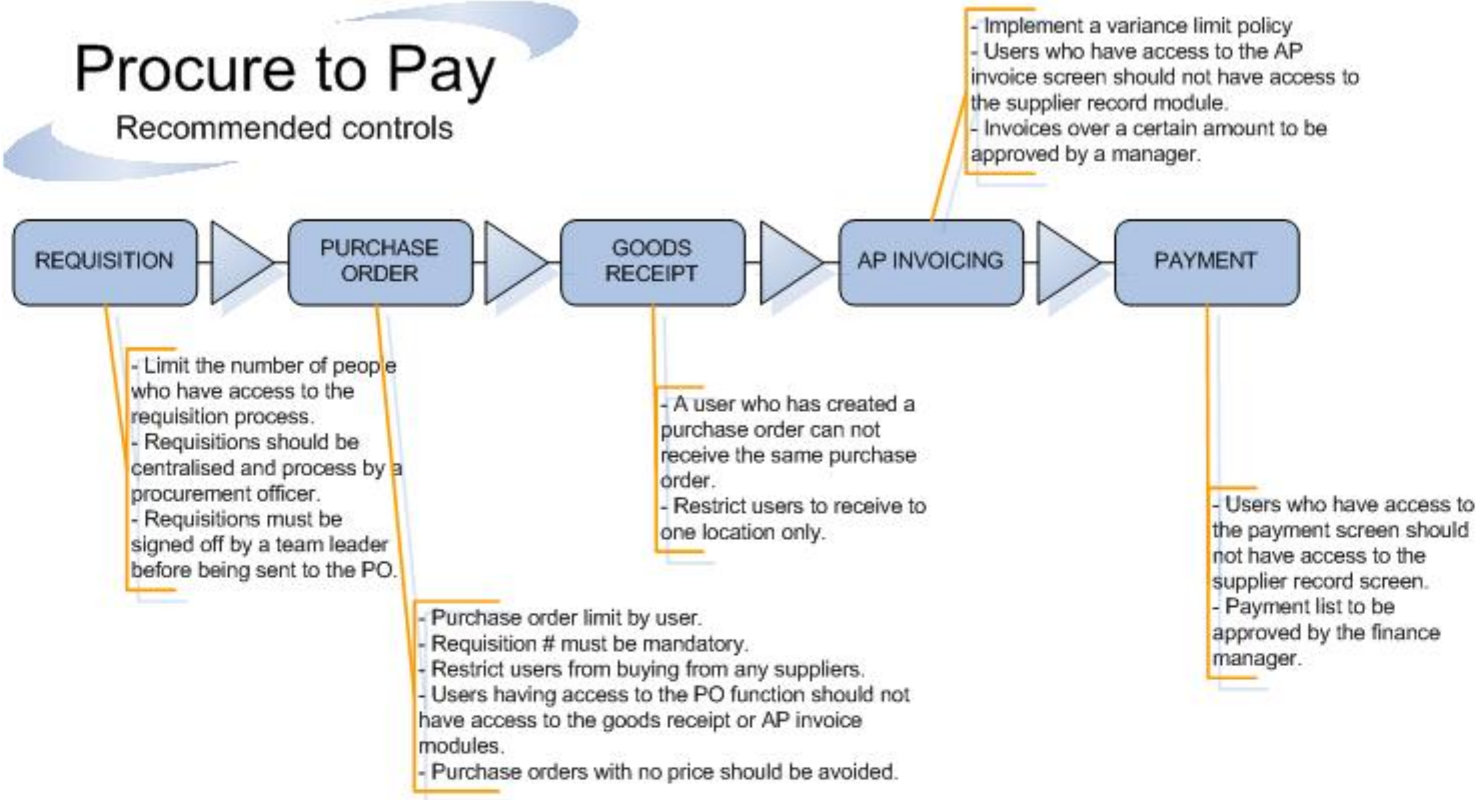
Maintaining SOD

Prevention

- Business Process Owners work in conjunction with I.T. setting up new user roles

Detection

- Internal audit
- Periodic evaluation and monitoring
- Automated ERP system tools



Procure to Pay

Recommended controls

- Limit the number of people who have access to the requisition process.
- Requisitions should be centralised and process by a procurement officer.
- Requisitions must be signed off by a team leader before being sent to the PO.

- Purchase order limit by user.
- Requisition # must be mandatory.
- Restrict users from buying from any suppliers.
- Users having access to the PO function should not have access to the goods receipt or AP invoice modules.
- Purchase orders with no price should be avoided.

- A user who has created a purchase order can not receive the same purchase order.
- Restrict users to receive to one location only.

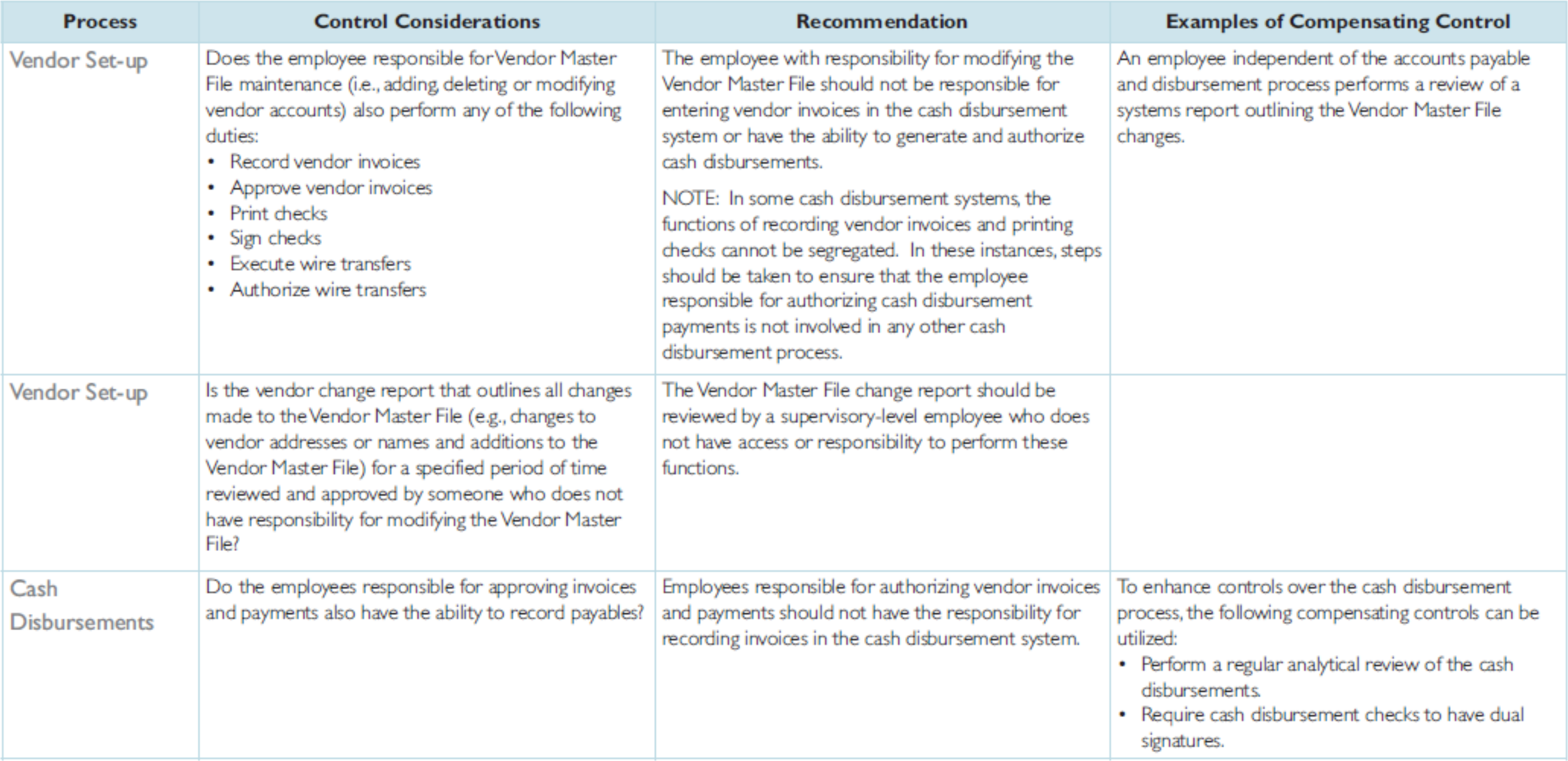
- Implement a variance limit policy
- Users who have access to the AP invoice screen should not have access to the supplier record module.
- Invoices over a certain amount to be approved by a manager.

- Users who have access to the payment screen should not have access to the supplier record screen.
- Payment list to be approved by the finance manager.

Specific examples of segregation of duties are as follows:

- The person who requisitions the purchase of goods or services should not be the person who approves the purchase.
- The person who approves the purchase of goods or services should not be the person who reconciles the monthly financial reports.
- The person who approves the purchase of goods or services should not be able to obtain custody of checks.
- The person who maintains and reconciles the accounting records should not be able to obtain custody of checks.

SOD Considerations In AP Process



Process	Control Considerations	Recommendation	Examples of Compensating Control
Vendor Set-up	Does the employee responsible for Vendor Master File maintenance (i.e., adding, deleting or modifying vendor accounts) also perform any of the following duties: • Record vendor invoices • Approve vendor invoices • Print checks • Sign checks • Execute wire transfers • Authorize wire transfers	The employee with responsibility for modifying the Vendor Master File should not be responsible for entering vendor invoices in the cash disbursement system or have the ability to generate and authorize cash disbursements. NOTE: In some cash disbursement systems, the functions of recording vendor invoices and printing checks cannot be segregated. In these instances, steps should be taken to ensure that the employee responsible for authorizing cash disbursement payments is not involved in any other cash disbursement process.	An employee independent of the accounts payable and disbursement process performs a review of a systems report outlining the Vendor Master File changes.
Vendor Set-up	Is the vendor change report that outlines all changes made to the Vendor Master File (e.g., changes to vendor addresses or names and additions to the Vendor Master File) for a specified period of time reviewed and approved by someone who does not have responsibility for modifying the Vendor Master File?	The Vendor Master File change report should be reviewed by a supervisory-level employee who does not have access or responsibility to perform these functions.	
Cash Disbursements	Do the employees responsible for approving invoices and payments also have the ability to record payables?	Employees responsible for authorizing vendor invoices and payments should not have the responsibility for recording invoices in the cash disbursement system.	To enhance controls over the cash disbursement process, the following compensating controls can be utilized: • Perform a regular analytical review of the cash disbursements. • Require cash disbursement checks to have dual signatures.

Question?

How many organizations have appropriate segregation of duties in their ERP application?

Answer:

Almost

NONE

Challenges in Auditing ERP Security

- The complexity of ERP systems leads to security vulnerabilities.
- There is a shortage of staff members trained in ERP security.
  - Able to interpret security permissions ("What does Qx14r22 grant access to?")
  - With a knowledge of business processes and needs
- Implementers commonly pay inadequate attention to ERP security during deployment (at the hiring companies' request).
- ERP customizations often inhibit the development of standardized security solutions.

The SOD Road Map

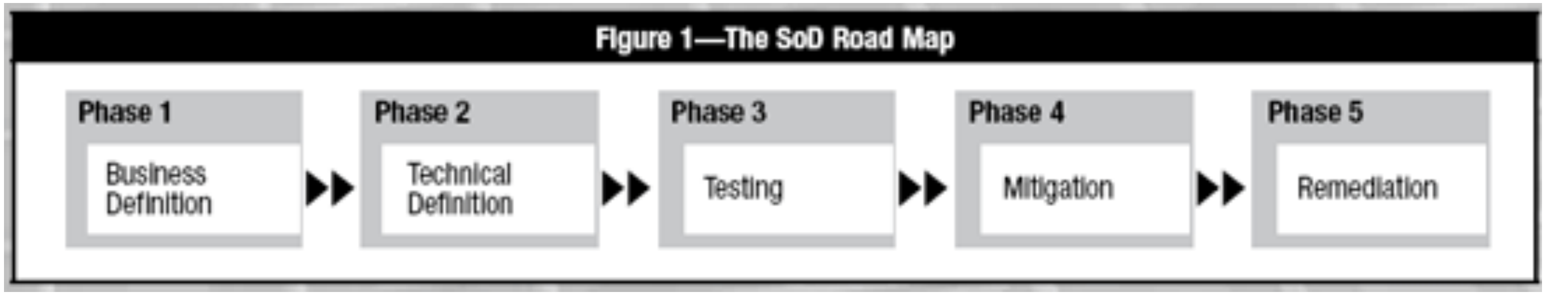


Figure 1—The SoD Road Map

Business Definition - The objective of this phase is to gain an understanding of the scope of sensitive transactions and conflicts that drive the company's key business processes. These are the transactions that pose the greatest fraud risk to the organization should someone possess excessive access.

Technical Definition - The technical definition uses the completed conflict matrix as a tool to help answer the question

Testing - Draws on data from the business definition and technical definition phases to produce an analysis of users with SOD conflicts.

The SOD Road Map (CONT)

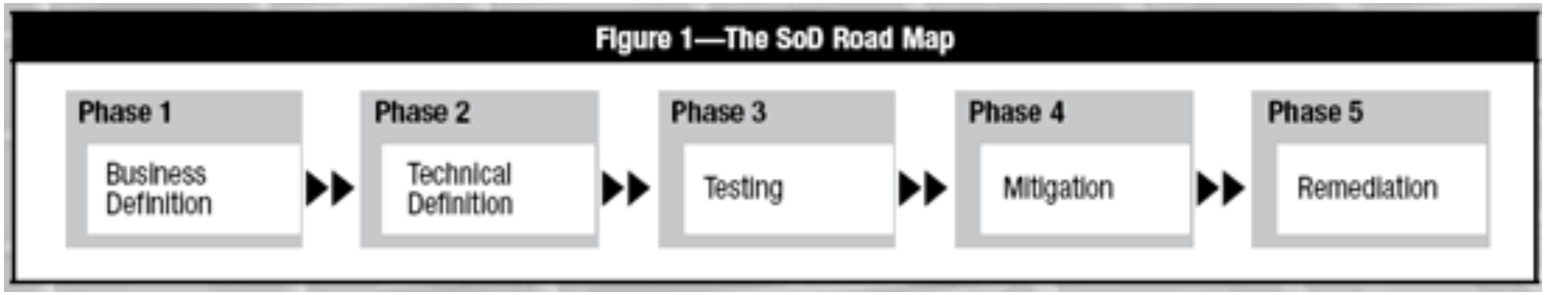


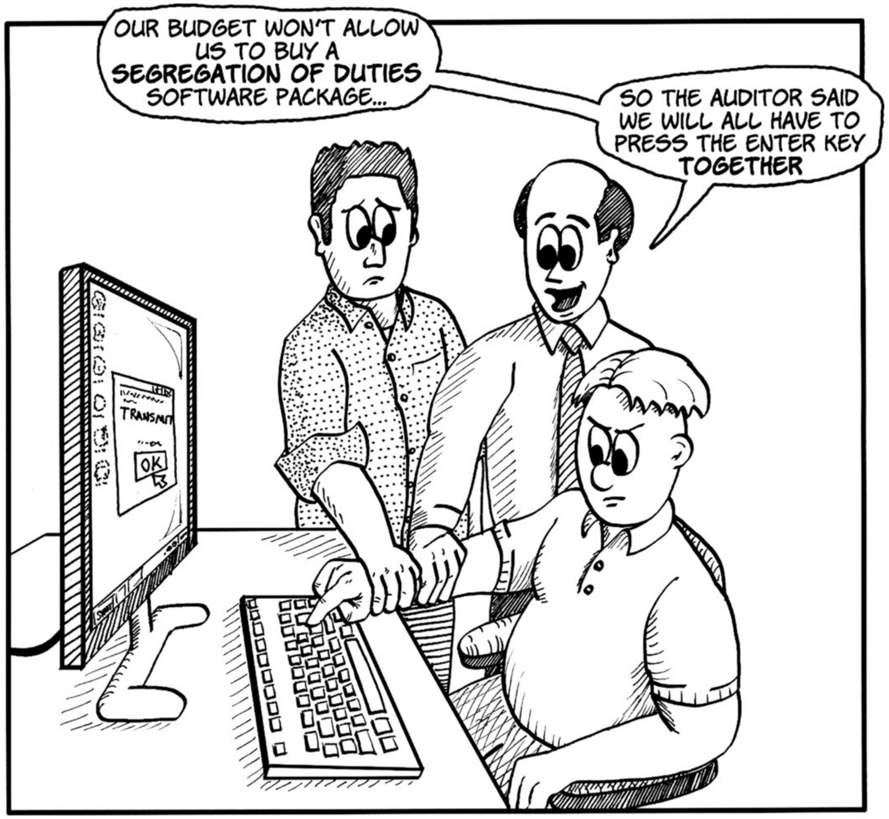
Figure 1—The SoD Road Map

Phase 1 Business Definition ▶▶ Phase 2 Technical Definition ▶▶ Phase 3 Testing ▶▶ Phase 4 Mitigation ▶▶ Phase 5 Remediation

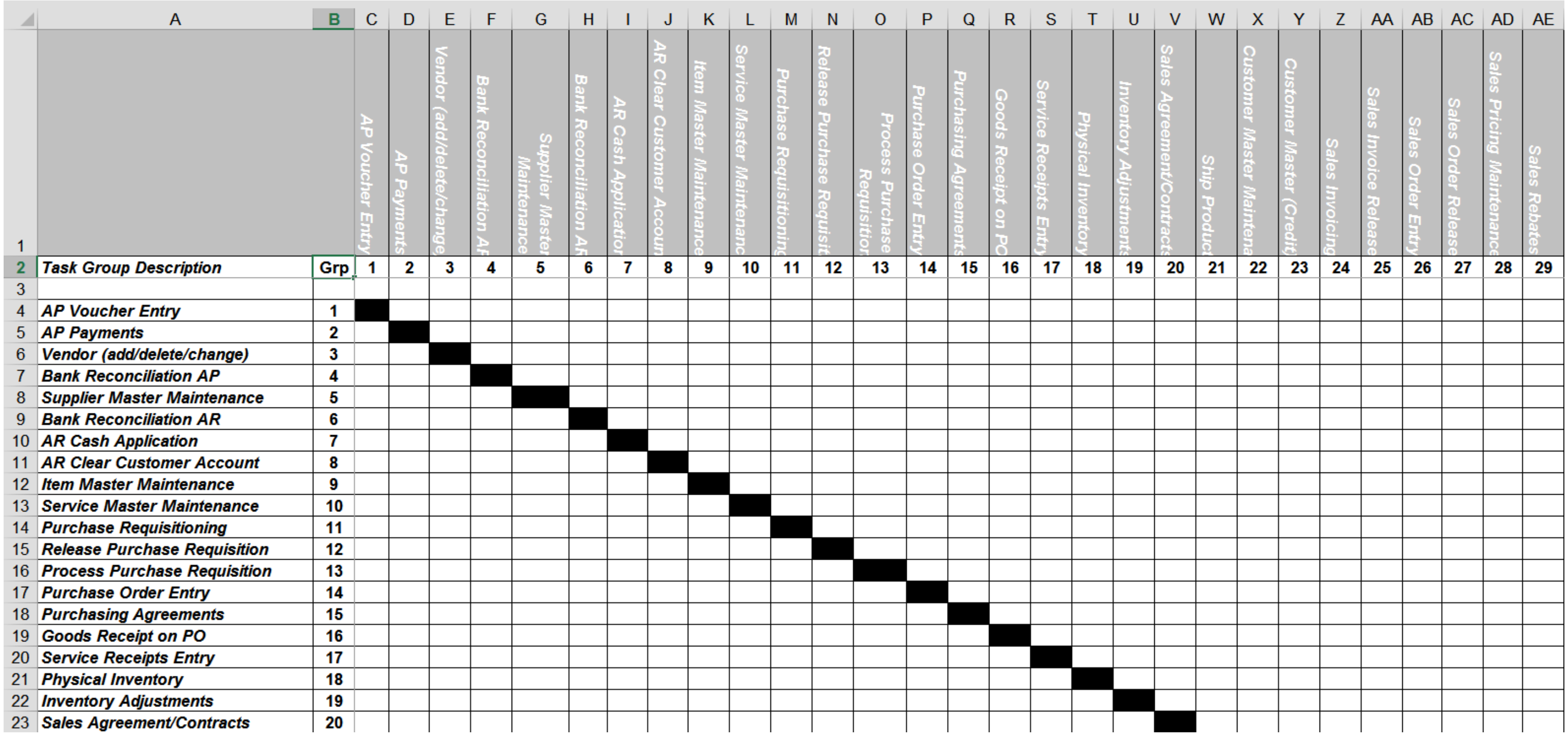
Mitigation - examines each of the identified SOD conflicts and asks, “Which effective financial controls (generally evidenced via testing documentation as part of a Sarbanes-Oxley initiative) can be cited to demonstrate that the residual risk of a particular SOD conflict does not pose a financially significant threat to the business?”

Remediation - Permanent correction of SOD conflicts.

MORE AUDIT HUMOR (**AUDIENCE SHOULD BE LAUGHING**)


OUR BUDGET WON'T ALLOW US TO BUY A SEGREGATION OF DUTIES SOFTWARE PACKAGE...
SO THE AUDITOR SAID WE WILL ALL HAVE TO PRESS THE ENTER KEY TOGETHER
TRANSMIT
OK

SOD MATRIX SAMPLE



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE
1			AP Voucher Entry	AP Payments	Vendor (add/delete/change	Bank Reconciliation AF	Supplier Master Maintenance	Bank Reconciliation AF	AR Cash Applicatior	AR Clear Customer Accoun	Item Master Maintenance	Service Master Maintenanc	Purchase Requisitioning	Release Purchase Requisit	Process Purchase Requisitior	Purchase Order Entry	Purchasing Agreements	Goods Receipt on PO	Service Receipts Entry	Physical Inventory	Inventory Adjustments	Sales Agreement/Contracts	Ship Product	Customer Master Maintena	Customer Master (Credit)	Sales Invoicing	Sales Invoice Release	Sales Order Entry	Sales Order Release	Sales Pricing Maintenance	Sales Rebates
2	*Task Group Description*	Grp	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
3																															
4	*AP Voucher Entry*	1	■																												
5	*AP Payments*	2		■																											
6	*Vendor (add/delete/change)*	3			■																										
7	*Bank Reconciliation AP*	4				■																									
8	*Supplier Master Maintenance*	5					■																								
9	*Bank Reconciliation AR*	6						■																							
10	*AR Cash Application*	7							■																						
11	*AR Clear Customer Account*	8								■																					
12	*Item Master Maintenance*	9									■																				
13	*Service Master Maintenance*	10										■																			
14	*Purchase Requisitioning*	11											■																		
15	*Release Purchase Requisition*	12												■																	
16	*Process Purchase Requisition*	13													■																
17	*Purchase Order Entry*	14														■															
18	*Purchasing Agreements*	15															■														
19	*Goods Receipt on PO*	16																■													
20	*Service Receipts Entry*	17																	■												
21	*Physical Inventory*	18																		■											
22	*Inventory Adjustments*	19																			■										
23	*Sales Agreement/Contracts*	20																				■									

Things To Remember

- Segregation of Duties helps prevent fraud and errors
- Companies should identify their SOD risks and controls
- A process is needed to correct ineffective SOD
- Maintaining effective SOD requires processes and tools
- Management is always surprised about current access
- Without performing an analysis, SOD issues are apparent after something bad occurs

Q & A

armanino

Armanino^{LLP} Certified Public Accountants & Consultants

Steve Shofner	office: 925.790.2879	mobile: 510.681.6638	email: steve.shofner@amllp.com
Junior DeAlba	office: 925.790.2719	mobile: 510.314.9306	email: Junior.DeAlba@amllp.com