

# The Importance of Segregation of Duties in Your ERP

Hilary Cabodi

Larry Best

February 15, 2023



The Association of  
Accountants and  
Financial Professionals  
in Business

ORACLE®  
NETSUITE

# Featured Presenters



**Hilary Cabodi**  
Managing Director  
Effectus Group



**Larry Best**  
Managing Director  
Effectus Group

# ABOUT US

Effectus is a national accounting advisory services firm headquartered in the San Francisco Bay Area

- The firm is comprised of former Big 4 professionals that were rated as top performers
- Unparalleled IPO expertise gained through advising numerous companies through the traditional and SPAC IPO process
- Significant M&A due diligence, purchase accounting, and post-close integration experience
- Fastest growing accounting advisory services firm in the San Francisco Bay Area for the last three years
- The firm has advised hundreds of public, private, venture backed, and private equity owned companies



ORACLE  
NETSUITE

Alliance Partner

Expertise in  
ERP

## Technical Accounting and IPO/SPAC Prep Services

- Adoption of new revenue standard (ASC 606)
- Adoption of new leasing standard (ASC 842)
- SEC reporting and assistance in filings, including drafting forms S-1 and S-4 (including MD&A, F-page financials, key financial metrics, etc.)
- Technical accounting memos for debt and equity issuances
- Stock-based compensation (memos and calculations)
- Business combination accounting (purchase accounting memos, opening balance sheet, SEC pro formas, etc.)
- Financial statements and footnote preparation

## Transaction Advisory Services (TAS)

- Buy-side due diligence
- Financial and operational integration assistance
- Purchase accounting assistance
- Sell-side due diligence
- Carve-out assistance

## Financial Operations and Systems

- Risk Advisory and SOX services
- Managed accounting services/staff augmentation (MAS)
- System implementation (NetSuite, Zuora RevPro, etc.)

# Poll Question 1:

What role do you hold in your organization?

- a) Director
- b) Supervisor
- c) Manager
- d) Controller
- e) Senior Staff (CFO, VP etc.)
- f) Accountant-Analyst
- g) Staff
- h) Other

# Poll Question 1 Results: (Placeholder)

# WHAT IS SEGREGATION OF DUTIES?

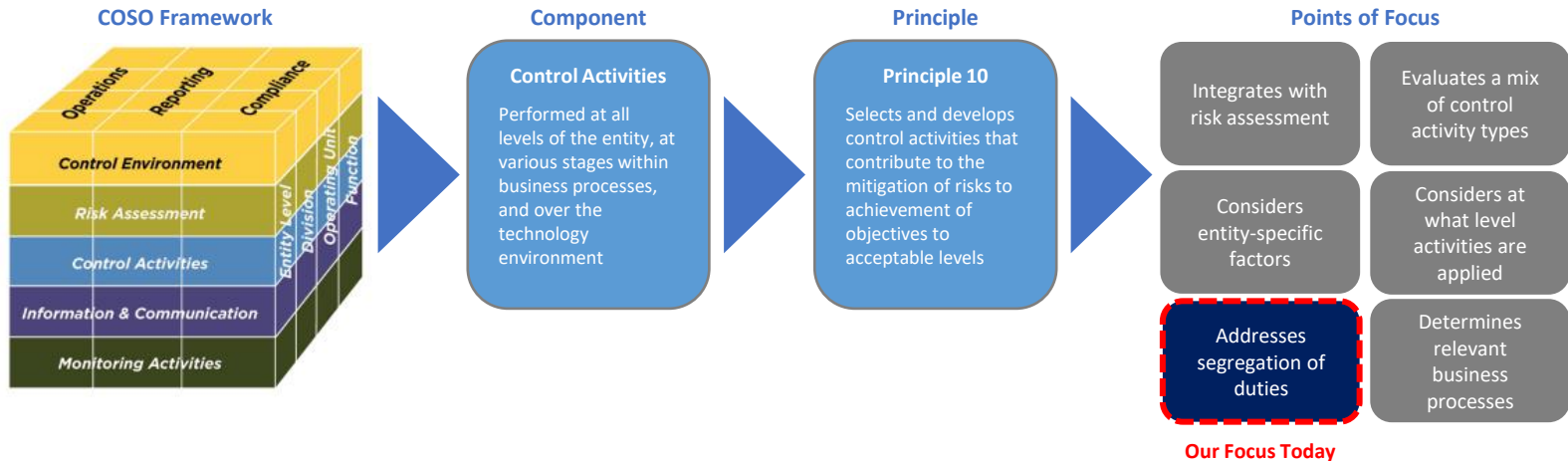
“Segregation of Duties (SOD) is a basic building block of sustainable risk management and internal controls for a business.”<sup>1</sup>

SOD is the concept of having more than one person required to complete a task. It is an administrative control used by organizations to prevent fraud, sabotage, theft, misuse of information, and other security compromises.

<sup>1</sup> As defined by the American Institute of Certified Public Accountants (AICPA)

# HOW DOES SEGREGATION OF DUTIES RELATE TO COSO?

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) Framework helps organizations design and implement internal control. The framework consists of 5 key components and 17 principles with points of focus highlighted for each principle. The correlation between SOD and COSO is as follows:



# IMPORTANCE OF SEGREGATION OF DUTIES

Segregation of duties is an essential element of control activities and is critical to an effective internal control environment as it is intended to:

1

**Detect Fraud**

**Reduce risk of fraudulent activities and inappropriate actions**

2

**Provide Oversight**

**Provide oversight and review to identify and resolve errors**



# COMPONENTS OF SEGREGATION OF DUTIES

When considering segregation of duties, it is important to separate the four components of duties and responsibilities.

Component	Authorization	Custody	Recordkeeping	Reconciliation
Description	The process of approving/authorizing transactions	Having access to or control over any physical asset	The process of creating and maintaining accounting records of different transactions	Verifying transactions to ensure that all transactions are valid and properly authorized
Examples	<ul style="list-style-type: none"> <li>• Verifying cash collections and daily balancing reports</li> <li>• Approving purchase requisitions/orders</li> <li>• Approving change orders, system design or programming changes</li> <li>• Approving time sheets, and payroll certifications</li> </ul>	<ul style="list-style-type: none"> <li>• Access to funds through the collection of funds, or processing of payments</li> <li>• Custodian of a petty cash or change fund</li> <li>• Receiving goods/services</li> <li>• Maintaining inventories</li> <li>• Handling or distributing paychecks/advice</li> </ul>	<ul style="list-style-type: none"> <li>• Preparing cash receipt back-ups or billings, purchase requisitions, payroll certifications, and leave records</li> <li>• Entering charges or posting payments to an A/R system</li> <li>• Maintaining inventory records</li> <li>• Recording journal entries</li> </ul>	<ul style="list-style-type: none"> <li>• Comparing billing documents to billing summaries</li> <li>• Comparing funds collected to accounts receivable postings</li> <li>• Comparing collections to deposits</li> <li>• Comparing payroll certifications to payroll summaries</li> </ul>

# EXAMPLES OF INCOMPATIBLE COMPONENTS

Examples of segregation of duties conflicts due to incompatible components and duties.

#	Example Responsibilities	Incompatible Components
1	<b>Authorizing a transaction</b> and <u>receiving and maintaining custody of the asset</u> that resulted from the transaction	<b>Authorization</b> and <u>Custody</u>
2	<b>Approving write-off of receivables</b> and <u>receiving funds (checks or cash)</u>	<b>Authorization</b> and <u>Custody</u>
3	<b>Reconciling bank statements/accounts</b> and <u>booking entries to general ledger</u>	<b>Reconciliation</b> and <u>Recordkeeping</u>
4	<b>Reconciling bank statements</b> and <u>depositing cash</u>	<b>Reconciliation</b> and <u>Custody</u>
5	<b>Approving time-cards</b> and having <u>custody of pay checks</u>	<b>Authorization</b> and <u>Custody</u>

## Poll Question 2:

Which Finance/ERP platform do you currently utilize:

- a. NetSuite
- b. QuickBooks
- c. Intacct/Xero
- d. Navision/Great Plains (Microsoft)
- e. Other - small-biz
- f. Other - mid-market
- g. Other - enterprise

## Poll Question 2 Results: (Placeholder)

# SEGREGATION OF DUTIES: 4 STEP PROCESS

The process to achieve segregation of duties can be broken into four steps.



# SOD PROCESS: UNDERSTAND



- Understand the roles and responsibilities of employees from various functions
- Identify the applications which are used by employees to carry out their roles and responsibilities
- Understand the ERP roles assigned to employees \*

*\* Most ERP systems leverages role-based security to provide users access to the application. Roles are granted to authorized personnel according to their job duties and each role is comprised of permissions for activities in the application.*

# SOD PROCESS: ANALYZE



- Generate an active employee listing
- Identify the users including assigned roles and access
- Analyze the number of roles assigned to each active employee
- Review whether the roles are appropriate for the employee's job responsibilities

# SOD PROCESS: IDENTIFY



- Identify conflicts in the roles and responsibilities
- Identify the associated risks for each conflict



# SOD PROCESS: IDENTIFY

A segregation of duties matrix is a tool to identify conflicts across roles and responsibilities for a particular area.

**Legend:**  
**Black** = Function 1 is the same as Function 2, no SOD noted  
**Green** = Function 1 and 2 create a conflict; IA performed testing and noted no user conflicts (click on the highlighted cell to be redirected to the testing performed)  
**Red** = Function 1 and 2 create a conflict; IA performed testing and noted one or more user conflicts (click on the highlighted cell to be redirected to the testing performed)  
**Blank** = Function 1 and 2 do not create a conflict

	Access and/or Custody to Fixed Assets	Access and/or Custody to Inventory	Access to Cash	Administer Security	Administrative Rights	Approve Journal Entries	Authorize Inventory or Expenditure Purchases	Block and Release Invoices	Create Payments	Create Purchase Order	Create Sales Orders	Deposit Cash Receipts	Edit Fixed Asset Master
Edit Fixed Asset Master													
Edit Inventory Master File		Green											
Create Journal Entries						Red							
Initiate Purchase of Fixed Assets													Green
Initiate Purchase of Inventory													
Initiate Purchase of Inventory and/or Expenditure Purchases							Green						
Inventory Count Responsibility		Green											
Investigate Discrepancies or Issues - Inventory		Green											
Investigate Inventory Count Discrepancies		Green											

# SOD PROCESS: IDENTIFY

A segregation of duties matrix is a tool to identify conflicts across roles and responsibilities for a particular area.

Sub-Process	#	Process Activity	Responsibility						Duties appear to be segregated?
			NetSuite Admin	Senior Global GL Accountant	Sr. Accounting Manager	Director of Technical Accounting & SEC Reporting or Designee	VP, Corporate Controller	CFO	
Policies & Procedures	1	Prepare and update accounting policies			x				Yes
		Review and approve accounting policies				x			
Chart of Accounts	2	Request changes to the Chart of Accounts			x				Yes
		Approve and review changes to the Chart of Accounts					x		
		Make changes in NetSuite per the approval	x				x		
Journal entries	3	Prepare a journal entry		x					Yes
		Approve and post a journal entry			x		x		
	4	Prepare accounting memos		x	x				Yes
		Review and approve accounting memos					x		
Period end close process	5	Perform task per the month-end close checklist		x					Yes
		Review completed task independently per the month-end			x		x		
	6	Prepare Account Reconciliation		x					Yes
		Review and approve Account Reconciliation			x		x		
	7	Prepare consolidation			x				Yes
		Review and approve consolidation					x		
	8	Request to reopen a closed accounting period		x					Yes
		Approve reopening of a closed accounting period					x		
Open a closed accounting period in NetSuite		x				x			
Financial statement preparation	9	Prepare monthly financial package		x	x				Yes
		Review and approve monthly financial package					x		
	10	Prepare SEC Filing Schedule/ Calendar					x		Yes
		Review and approve SEC Filing Schedule/ Calendar						x	
	11	Prepare 10Q/10K including EPS calculation				x			Yes
		Review and approve 10Q/10K EPS calculation						x	
Issue or file 10Q/10K review including EPS calculation					x				
12	Prepare relevant disclosures				x			Yes	
	Review and approve relevant disclosures					x			

# SOD PROCESS: IDENTIFY

Segregation of duties software tools may be used to identify conflicts across roles and responsibilities as well.

Action Item	User Count	General Ledger Posting			Currency & Accounts	
	Only 4/22 roles are currently being used - it would be advised to inactivate any not being used and to deploy new roles with intent as the business expands	It is not recommended to delete transactions or master data, as such, FULL access should be granted sparingly, and perhaps removed entirely once the system matures.			It is not recommended to delete transactions or master data, as such, FULL access should be granted sparingly, and perhaps removed entirely once the system matures.	
Name		Journal Posting Risk	Journal Approval	Make Journal Entry	Accounts	Currency
Administrator	8	FALSE				
IB - A/P Analyst	0	FALSE		Create	View	
IB - A/R Analyst	0	FALSE		Edit	View	
IB - Accountants	2	TRUE	Full	Edit	Edit	
IB - Controller	1	TRUE	Full	Full	Full	Full
IB - Executive	3	FALSE	Full	Create	View	
IB - Inventory Manager	0	FALSE				
IB - Project Manager	0	FALSE				
IB - Purchasing	0	FALSE				
IB - Sales	0	FALSE				

# SOD PROCESS: ADDRESS



- Address conflicts by removing access and/or reassigning roles and responsibilities to a separate employee
- Identify mitigating controls which are in place and/or implement new mitigating controls for conflicts that can't be addressed due to resource constraints or system limitations

## Poll Question 3:

Do you currently leverage a Segregation of Duties software tool to perform your analysis?

- a) Yes
- b) No
- c) I don't know

## Poll Question 3 Results: (Placeholder)

# COMMON TOOLS USED TO AUTOMATE SOD ANALYSIS

- **Fastpath Assure** is a comprehensive, interactive tool that enables organizations to identify security conflicts within NetSuite, better understand their overall security and provide the necessary documentation to both internal and external audit teams.
- **Strongpoint** is a leading NetSuite-native solution for SOX compliance, SoD, change management and documentation tool.
- **Vibato** provides internal control solutions and comprehensive internal control procedures to help public, private, and nonprofit organizations improve their financial risk management and compliance efforts.
- **Saviynt Application Access Governance (AAG)** solution provides a preventive and detective SoD analysis capability, and out-of-the-box rulesets to provide a granular view of application risk to help maintain audit readiness with continuous compliance across applications like SAP, Workday, Oracle, and other SaaS and on-premise applications.

# COMMON ROLES IN ERP SYSTEMS

Examples of common roles that are typically included in ERP systems:

Roles	Role Description
Administrator	Has all permissions in the ERP account at all levels
Accounts Payable Accountant	Has permissions in accounts payable and expense management
Accounts Receivable Accountant	Has permissions in accounts receivable management
Accountant/Bookkeeper/Controller	Has permissions in bookkeeping and reporting modules
Human Resource Generalist/Payroll Manager	Has permissions in HR modules



# EXAMPLES OF COMMON CONFLICTS IN ERP ROLES

Examples of common segregation of duties conflict (with associated risks) in ERP systems:

1

**Creation of vendors AND bill payments to vendors**

Risk of unauthorized or fraudulent payments made to vendors

3

**Creation AND approval of purchase requests**

Risk of unauthorized or fraudulent purchases

2

**Creation of customers AND issuance of credit memos to customers**

Risk of unauthorized or fraudulent credits issued to customers

4

**Creation of AND approval of journal entries**

Risk of unauthorized or fraudulent transactions recorded in the G/L

# ADDRESS SOD ISSUES IN ERP SYSTEMS

Procedures to minimize the risks of segregation of duties issues in ERP systems:



Review users with multiple roles and consider assigning one role for every user ensuring there are no permission conflicts in the role



Analyze permissions for active users to determine whether conflicts exist



Review the permission for each role before assigning multiple roles to a user



Identify mitigating controls which are in place and/or implement new mitigating controls for conflicts that can't be addressed due to resource constraints or system limitations

## Poll Question 4:

How often does your organization perform a segregation of duties analysis?

- a) Quarterly
- b) Annually
- c) Every other year
- d) Once
- e) Never

## Poll Question 4 Results: (Placeholder)

# CASE STUDY

Situation	A publicly traded company shifted from QuickBooks and implemented NetSuite for their ERP and requested an assessment of user roles and responsibilities.
Task	In accordance with SOX compliance, Effectus Group performed a SOD analysis of the company's GL module in NetSuite to identify conflicts related to the financial close process.
Action	<ul style="list-style-type: none"><li>• Using a proprietary tool, Effectus Group analyzed the company's user access for the GL module and identified segregation of duties violations.</li><li>• Each violation was reviewed with management to verify results.</li><li>• Action plans were communicated to management for resolution.</li></ul>
Result	<ul style="list-style-type: none"><li>• Reduced risk</li><li>• Segregated roles and responsibilities</li><li>• Compliance with SOX</li></ul>

# CASE STUDY

Summary of observations and recommended actions are presented to and discussed with management.

EFFECTUS GROUP		NetSuite SOD Roles & Permissions Analysis	
Area Assessed	Flag ID	Observations	Recommended Action
General System Configuration	SC01	There are currently 22 roles which can be selected and assigned to new and existing users. Of those, only 3 + Administrator are being used.	Inactivate all roles except: - Administrator - IB - Accountants - IB - Controller - IB - Executive
	SC02	There are currently 8 active administrators on the account. Of these: - 4 are NetSuite ACS/PS users	Once implementation has been finalized, it is recommended to reduce admin access to two (2) internal company employees.
	SC03	Many roles have FULL access on transaction and master data records (eg. Subsidiary, GL Account, Department, Class, Location, Employee, Customer Vendor)	While NetSuite has built-in controls which will prevent a record tied to posted financial history or <b>closed</b> accounting periods, it is still recommended that transactions are voided, and master data is inactivated when it is no longer in use. Reduce all FULL access permissions to EDIT.
	SC04	The <b>IB - Executive</b> role has Create, Edit & View permission for transactions and master data in the system.	Typically we recommend that unless there is a valid use case presented, executive users should be view only in the system. Reduce all Full, Edit and Create permissions for Transactions and master data to VIEW only.

# Questions and Answers



**Hilary Cabodi**  
Managing Director  
Effectus Group



**Larry Best**  
Managing Director  
Effectus Group

# Thank you!

Oracle NetSuite

<https://www.netsuite.com/>



The Association of  
Accountants and  
Financial Professionals  
in Business

**ORACLE®**  
**NETSUITE**