



# C24 - SEGREGATION OF DUTIES

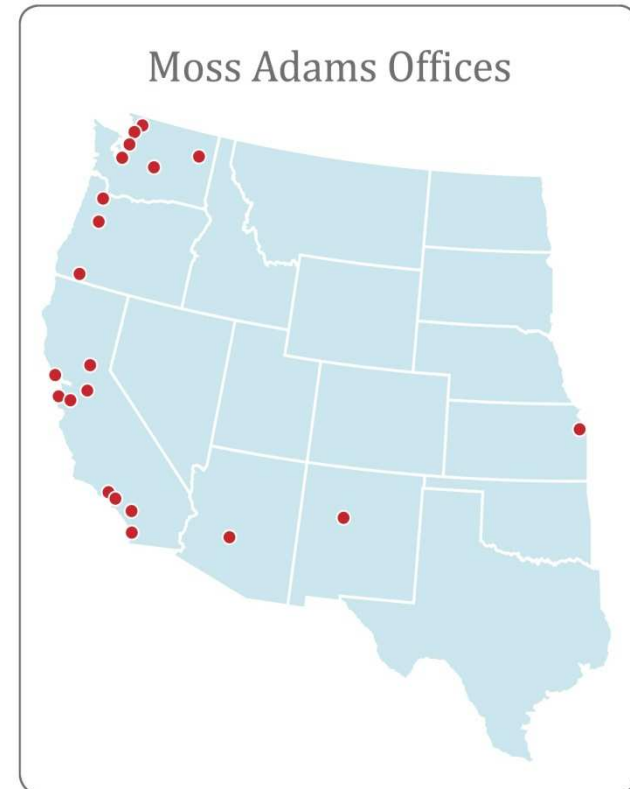
What's the Risk and What Do We Do  
About It?

Weston Nelson

*Back to Business*

# Moss Adams LLP

- 11<sup>th</sup> largest accounting and business consulting firm in the U.S.
- 21 locations; 1,800 personnel
- Industry-focused service groups
- IT consulting specialists



# Our Objectives

---

- Clarify the role of Segregation of Duties (SOD)
- How to implement effective SOD
- Clarify the evaluation process of current user access
- Identify alternatives to SOD
- Other SOD Considerations

# Agenda

---

- What is segregation of duties?
- Discuss fraud and risks of fraud
- Examples of SOD violations
- Demonstrate a method for evaluating SOD
- Considerations for maintaining proper SOD
- Questions / Answer

# What is Segregation of Duties?

---

- How do you define it?
- What is the goal of segregation of duties?
- Are all SOD conflicts equal in importance?



# What is Segregation of Duties? (cont.)

---

- COSO: “Dividing or allocating tasks among various individuals making it possible to reduce the risks of error and fraud.”
- Contains four components:
  - ❖ Custody
  - ❖ Authorization
  - ❖ Record keeping
  - ❖ Reconciliation

# What is Segregation of Duties? (cont.)

---

- Ideally, a single individual would have responsibility for only a single component.
- Benefits include:
  - ❖ Safeguarding of assets
  - ❖ Accurate financial reporting
  - ❖ Reduced risk of non-compliance
  - ❖ Reduced cost of compliance for automated SOD (e.g., SOX and external audit)



# What is Segregation of Duties? (cont.)

---

- SOD conflicts are not equally important to every company:
  - ❖ Safeguarding of assets vs. financial reporting risks
  - ❖ Relative importance of information confidentiality
  - ❖ Nature of company assets
  - ❖ Reduced risk when the “chain” of access is broken

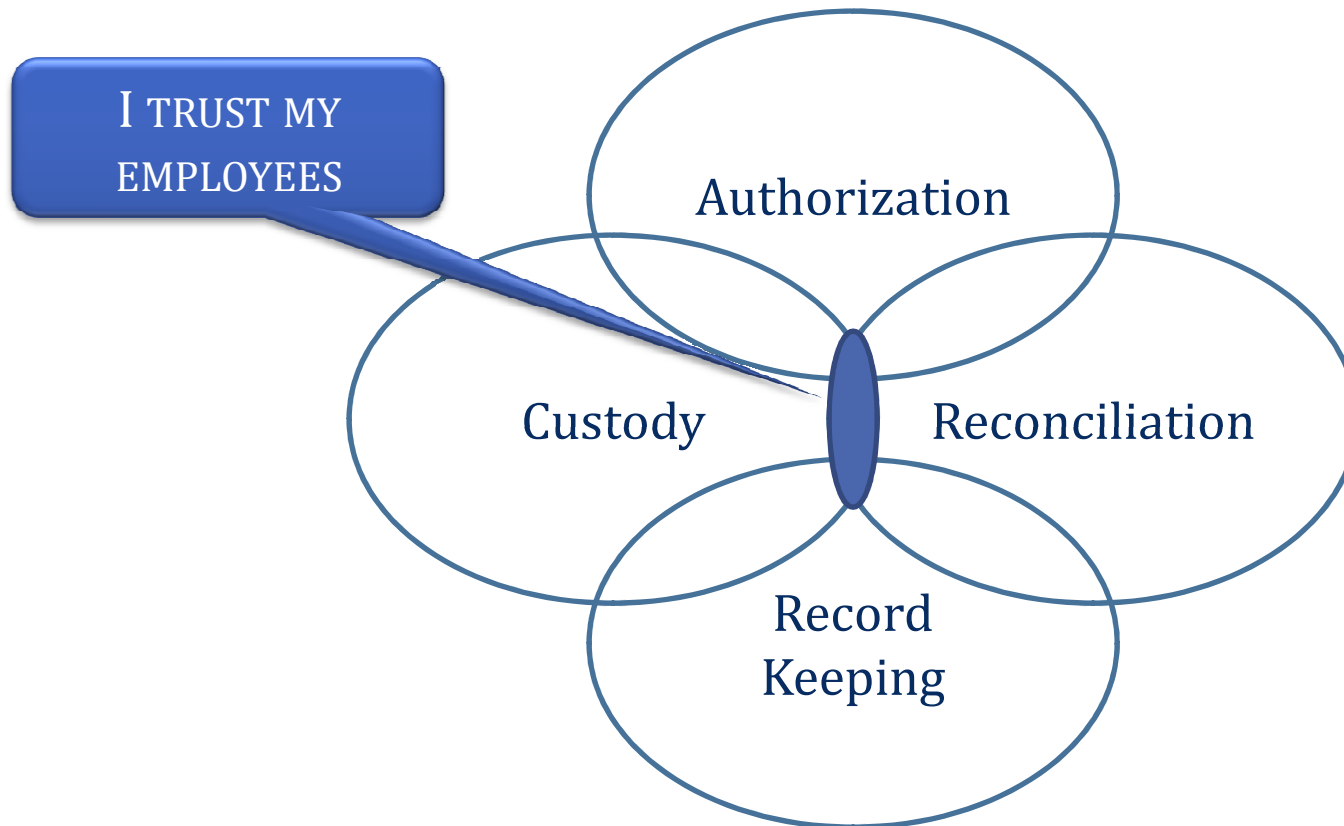


# Where Does Fraud Begin?

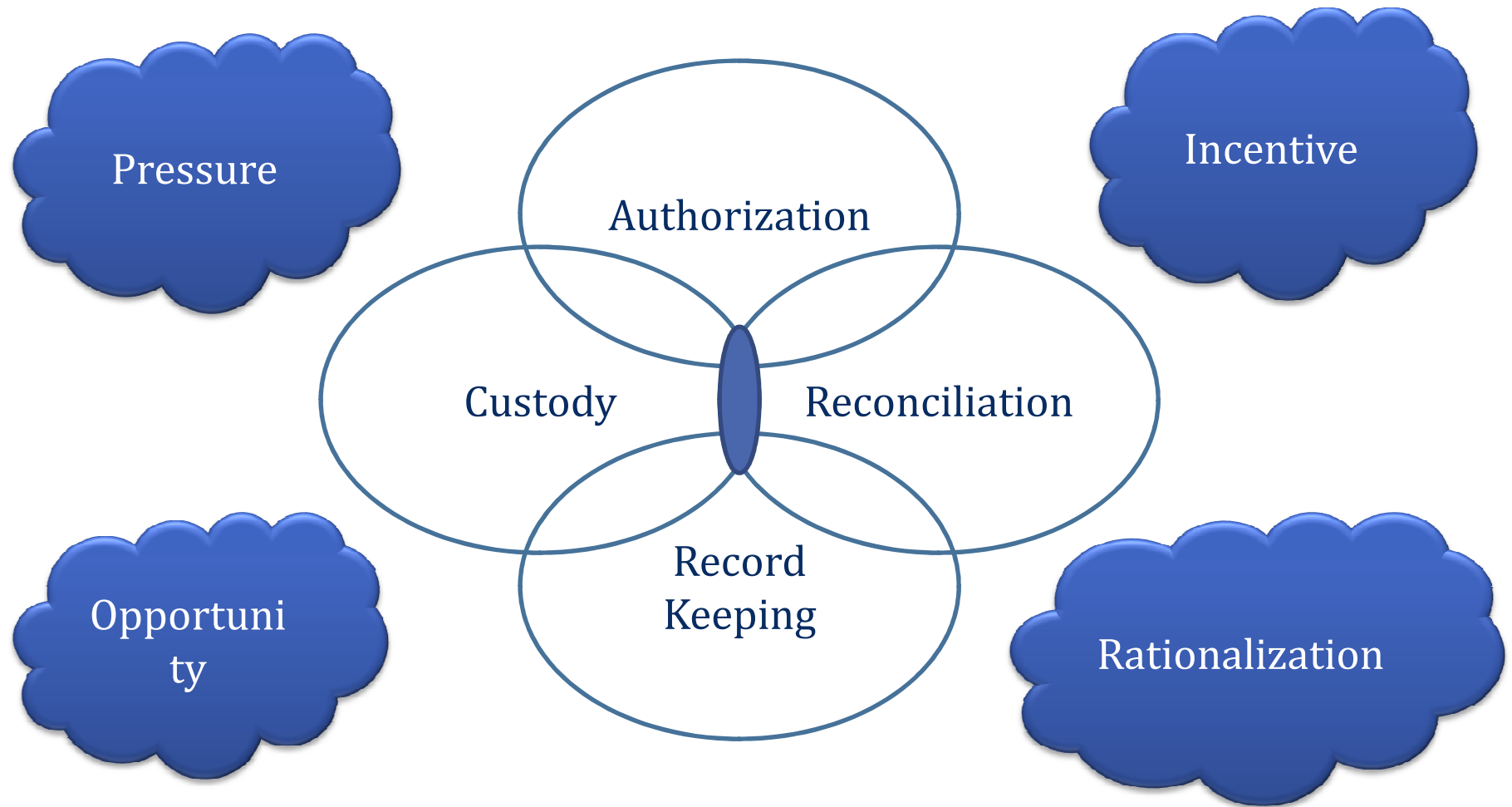
---



# Where Does Fraud Begin? (cont.)



# Where Does Fraud Begin? (cont.)



# Why do I care – examples in the news...

---

- NEC
  - Invalid revenue (\$18M) and kickbacks (\$4.2M)
- Société Générale
  - Unauthorized Trades (\$7B)
- Madoff
  - Ponzi scheme (\$50B)



# Management is Surprised...

---

- All 51 users in a Lawson implementation could enter and approve journal entries
- 21 users could enter/approve cash receipts, enter/approve journal entries and perform bank reconciliations

# Management is Surprised... (cont.)

---

- 105 users in a revenue related system could modify user security
- 223 users in a revenue system could modify the cash drawer beginning balance
- 316 users had access to virtually all sensitive transactions in a hospital revenue application

# Management is Surprised... (cont.)

---

- 3,100 KRONOS users could authorize their own payroll
  - ❖ 1,100 were hourly employees who could approve their own overtime
  - ❖ All 3,100 could change their own vacation accruals and approve payment in-lieu of vacation

# So Who owns SOD?

---

- Who owns segregation of duties
  - ❖ IT ?
  - ❖ The business ?
  
- Need for collaboration (both own it)
  - ❖ The business must own and define
  - ❖ IT must facilitate and enforce



# Evaluating Your SOD

---

- Define and create a policy or standard.
  - ❖ Include a statement that defines responsibility for enforcing the policy and maintaining proper SOD
  - ❖ Ultimately includes a list of incompatible duties
- Identify the core tasks performed at your company.

# Evaluating Your SOD (cont.)

---

- Identify incompatibilities.
  - ❖ Risk-based for your business
  - ❖ Consider “sensitive” duties such as posting of journal entries, performing reconciliations and Master Data files

# Example SOD Matrix

Sensitive Activities	Customer Master	Sales Order Entry/Edit	Sales Order Approval	Ship Confirm	Vendor Master	Requisition Entry/Edit	Requisition Approval	Purchase Order Entry/Edit	Purchase Order Approval	Receiving	Inventory Adjustment Entry
Customer Master	■	■									
Sales Order Entry/Edit	■	■	■	■							
Sales Order Approval		■	■								
Ship Confirm		■		■	■						■
Vendor Master				■	■			■			
Requisition Entry/Edit						■	■			■	
Requisition Approval						■	■				
Purchase Order Entry/Edit					■			■	■	■	
Purchase Order Approval								■	■		
Receiving						■		■		■	■
Inventory Adjustment Entry				■				■		■	■

# Evaluating Your SOD (cont.)

---

- Understand roles for key responsibilities – access rights or capabilities.
  - ❖ Shipping/receiving
  - ❖ Purchasing
  - ❖ Accounts Payable
  - ❖ Accounts Receivable
  - ❖ Vendor Master

# Evaluating Your SOD (cont.)

---

- Translate business tasks and activities into security and access rights within key applications.
  - ❖ How is access granted (e.g., roles, menus, objects, etc.)?
  - ❖ Define menus or objects granting user access.
  - ❖ Identify the “sensitive” objects associated with conflicting duties.

# Evaluating Your SOD (cont.)

Object	Description	Area
P0012	Automatic Accounting Instructions	AAI
P0022	Tax Rules	Tax
P0030G	G/L Bank Accounts	Accounting
P03013	Customer Master	Customer Master
P03B0001	Speed Receipts Entry	Receiving
P03B0002	Invoice Revisions	Vendor Invoices Entry/Edit
P03B102	Standard Receipt Entry	Receiving
P03B11	Standard Invoice Entry	Vendor Invoices Entry/Edit
P03B11SI	Speed Invoice Entry	Vendor Invoices Entry/Edit
P03B11Z1	Batch Invoice Revisions	Vendor Invoices Entry/Edit
P03B121	Work With Electronic Receipts Input	Receiving
P03B123	Electronic Receipt Entry	Receiving
P03B305	Credit Granting / Management	Customer Master
P03B42	A/R Deduction Activity Master Maintenance	Customer Master


Receiving Role

# Evaluating Your SOD (cont.)

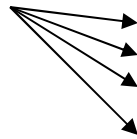

---

- Determine the existing role access rights.
  - ❖ Identify built-in conflicts provided by each role.
  - ❖ Document desired changes to roles.
- Determine the users assigned to roles.
  - ❖ Provide a complete list of user conflicts allowed.

# Evaluating Your SOD (cont.)



User	Role
User1	Receiving
User2	Receiving
User3	AP
User4	AP
User5	AR
User6	AR
User7	GL

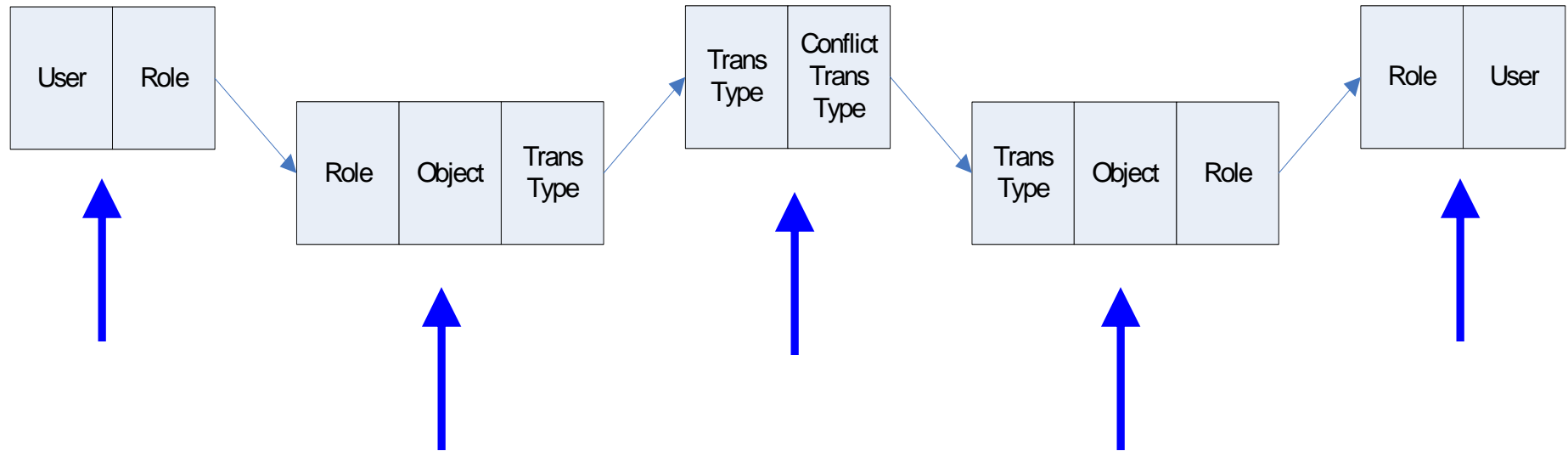



Role	Object	Description
GL	P0012	Automatic Accounting Instructions
GL	P0030G	G/L Bank Accounts
AR	P03013	Customer Master
AR	P03B305	Credit Granting/Management
AR	P03B42	A/R Deduction Activity Master Maintenance
Receiving	P03B0001	Speed Receipts Entry
Receiving	P03B102	Standard Receipt Entry
Receiving	P03B121	Work With Electronic Receipts Input
Receiving	P03B123	Electronic Receipt Entry
Tax	P0022	Tax Rules
AP	P03B0002	Invoice Revisions
AP	P03B11	Standard Invoice Entry
AP	P03B11SI	Speed Invoice Entry
AP	P03B11Z1	Batch Invoice Revisions

Tables such as the above will provide information of user access to sensitive transactions



# Evaluating Your SOD (cont.)



The above graphic depicts how user conflicts can be identified using lists of:

- Users/roles
- Roles/objects/transaction types
- Conflicting pairs of transaction types

# Evaluating Your SOD (cont.)

---

- Added requirements:
  - ❖ Roles should not contain “built-in” conflicts
- Additional issues and complexity:
  - ❖ Users assigned to multiple roles
  - ❖ Users assigned access rights by User ID
  - ❖ Users accessing multiple systems



# SOD Alternatives

---

- Does this solve all issues? Not likely.
  - ❖ Small groups of Users
  - ❖ System constraints
  - ❖ Manual activities outside the system
- Detective controls have a role.
  - ❖ Audit trails
  - ❖ Exception reports



# Other SOD Considerations

---

- IT activities creating an SOD concern:
  - ❖ Application administrator access
  - ❖ Security administrator and User setup
  - ❖ Programmer access to production
  - ❖ Powerful utilities
  - ❖ Strength of authentication
  - ❖ Shared passwords
  - ❖ Access to edit/change audit tables

# Maintaining SOD

---

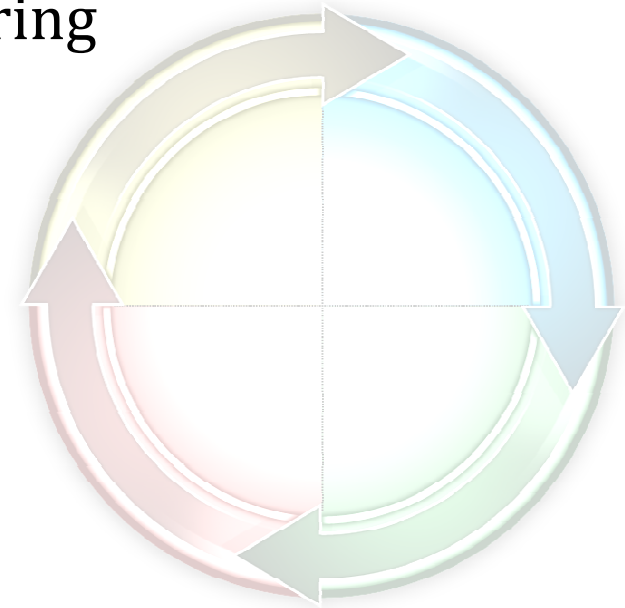
- Prevention
  - ❖ Tools for granting User access rights
    - IT becomes a gatekeeper
    - Conflicts raised for added approval or mitigation
  - ❖ Role and User change controls
  - ❖ Periodic User assessments and validation



# Maintaining SOD (cont.)

---

- Detection
  - ❖ Internal audit
  - ❖ Periodic evaluation and monitoring
  - ❖ Exception reporting
- Automated methods
  - ❖ Automated monitoring
  - ❖ ERP system tools and workflow



# Key Points

---

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

# Questions and Answers

---





# Thank You For Attending

---

Weston Nelson

Senior Manager, Business Risk Management

Weston.Nelson@mossadams.com

Office: (503) 478-2144