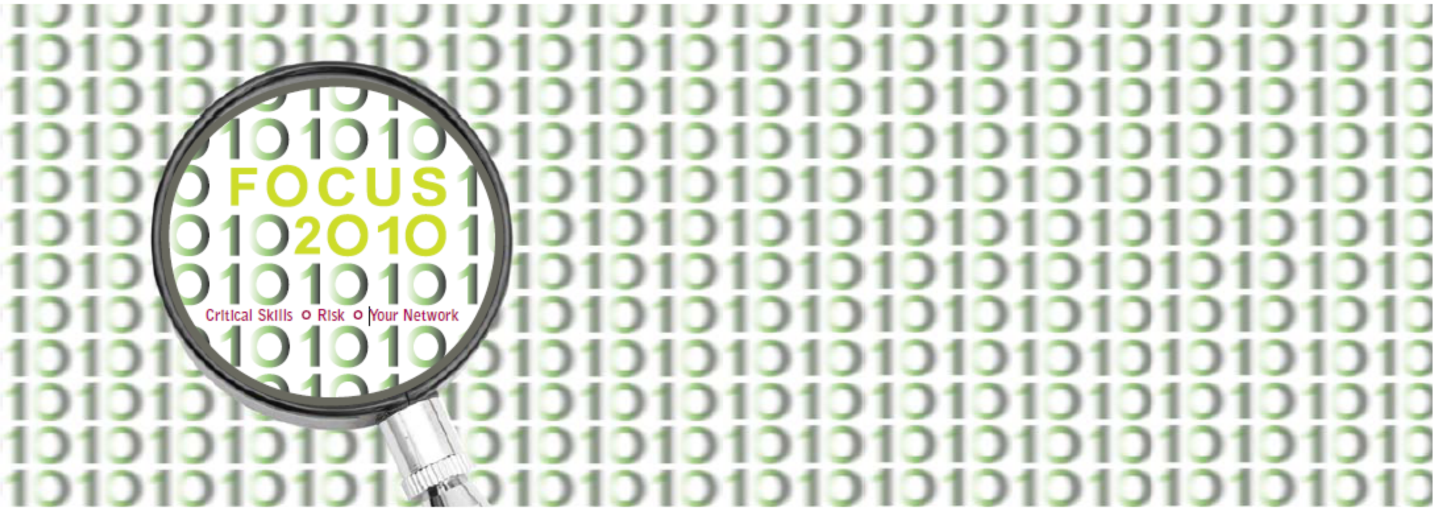
10th Annual SF ISACA Fall Conference

October 4 – 6, 2010



C23: Segregation of Duties: What's the Risk and What Do We Do About It?

Scott Mitchell and Eric Miles,
Moss Adams LLP

ISACA®
Trust in, and value from, information systems
San Francisco Chapter

ISACA
Trust in, and value from, information systems
San Francisco Chapter

Segregation of Duties

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

FOCUS 2010
Critical Skills ○ Risk ○ Your Network

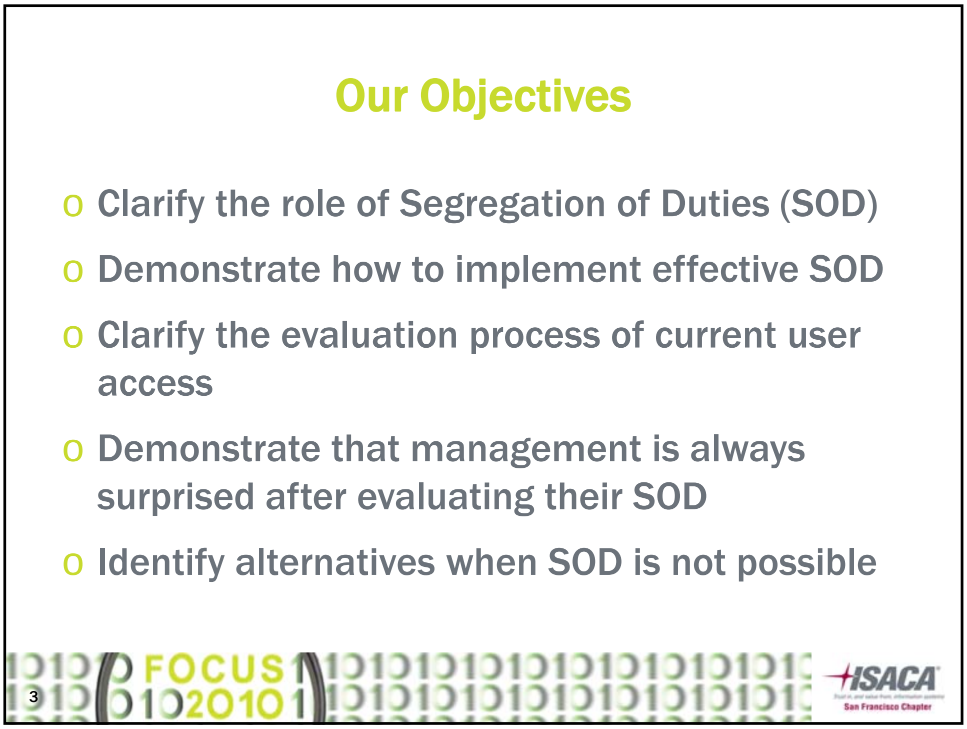
Moss Adams LLP

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

WASHINGTON
MONTANA
OREGON
IDAHO
WYOMING
NEVADA
UTAH
CALIFORNIA
COLORADO
ARIZONA
NEW MEXICO
TEXAS

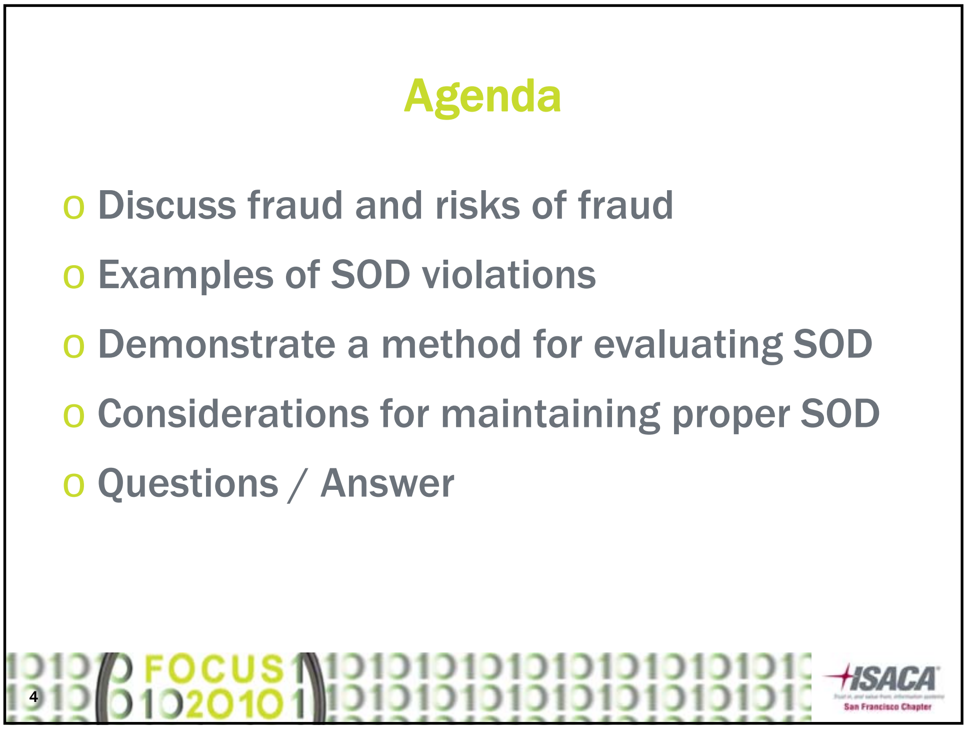
FOCUS 2010

ISACA
Trust in, and value from, information systems
San Francisco Chapter



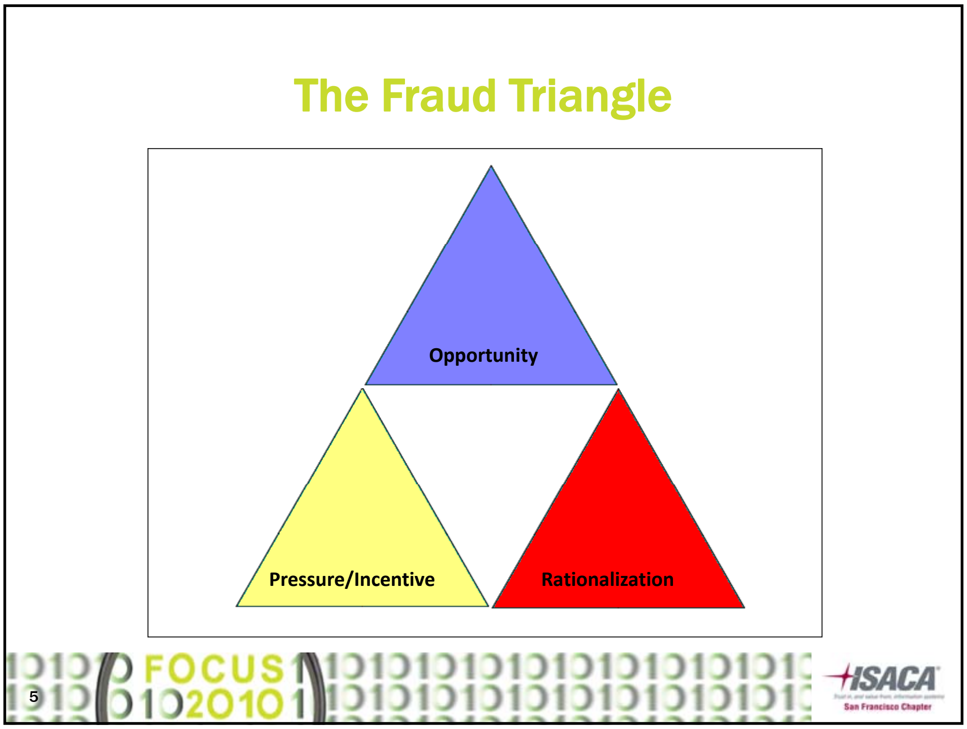
Our Objectives

- Clarify the role of Segregation of Duties (SOD)
- Demonstrate how to implement effective SOD
- Clarify the evaluation process of current user access
- Demonstrate that management is always surprised after evaluating their SOD
- Identify alternatives when SOD is not possible

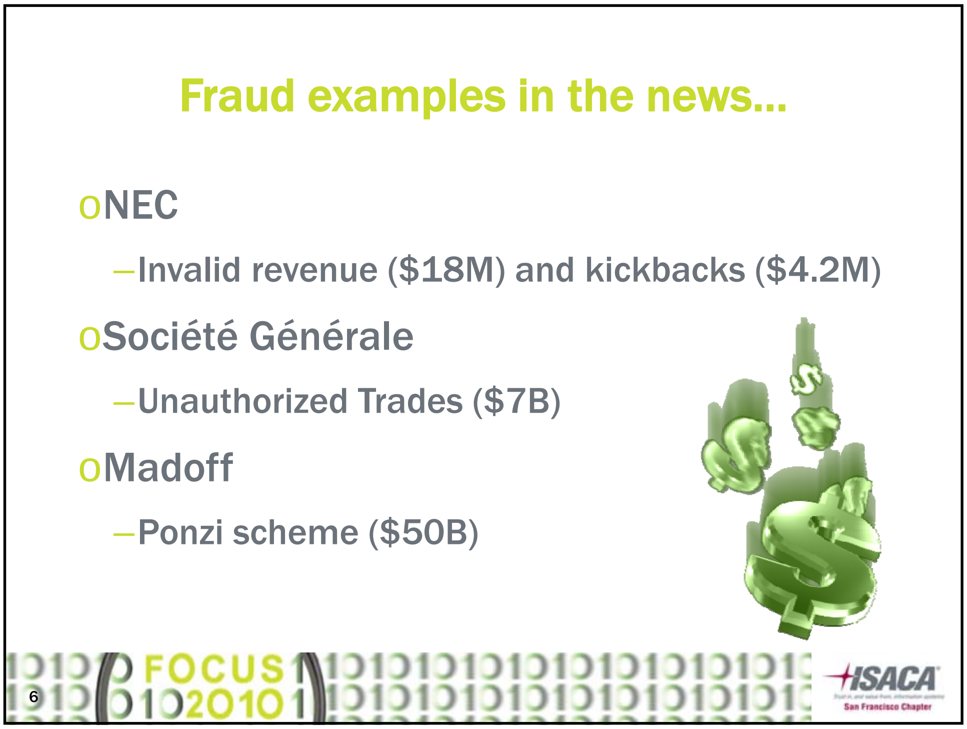


Agenda

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

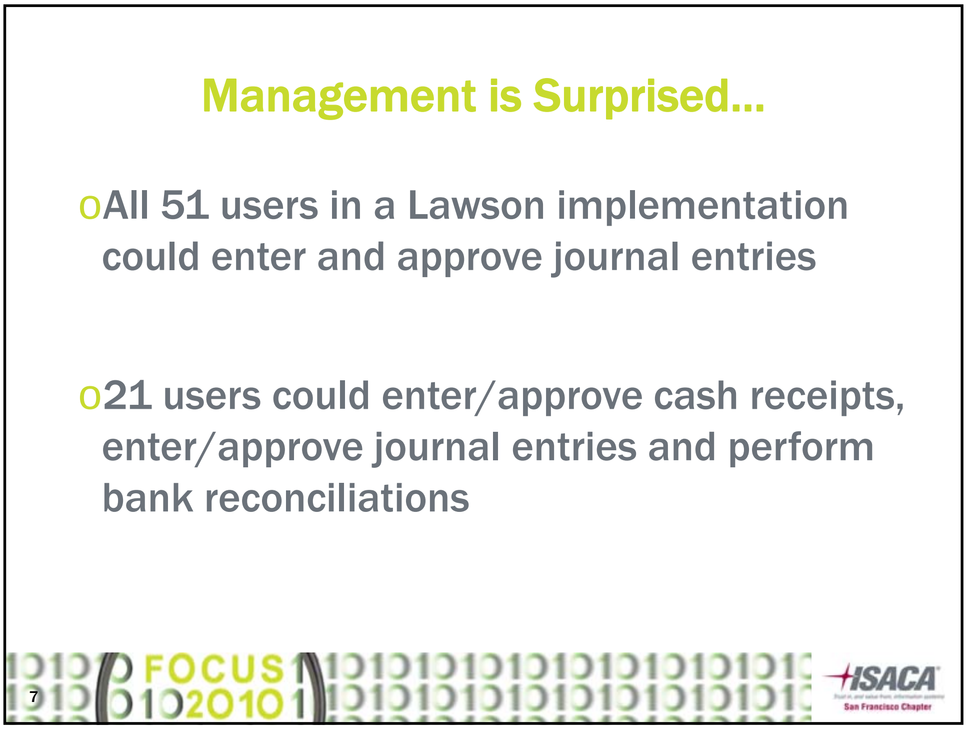


The Fraud Triangle



Fraud examples in the news…

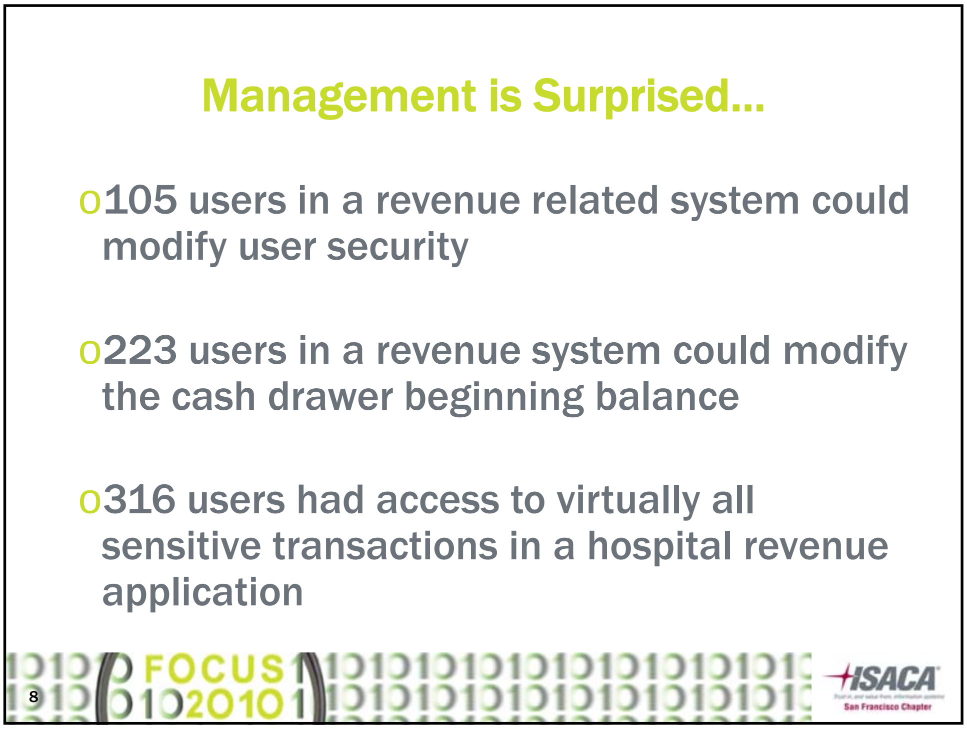
- NEC
  - Invalid revenue ($18M) and kickbacks ($4.2M)
- Société Générale
  - Unauthorized Trades ($7B)
- Madoff
  - Ponzi scheme ($50B)



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

7



Management is Surprised…

- 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

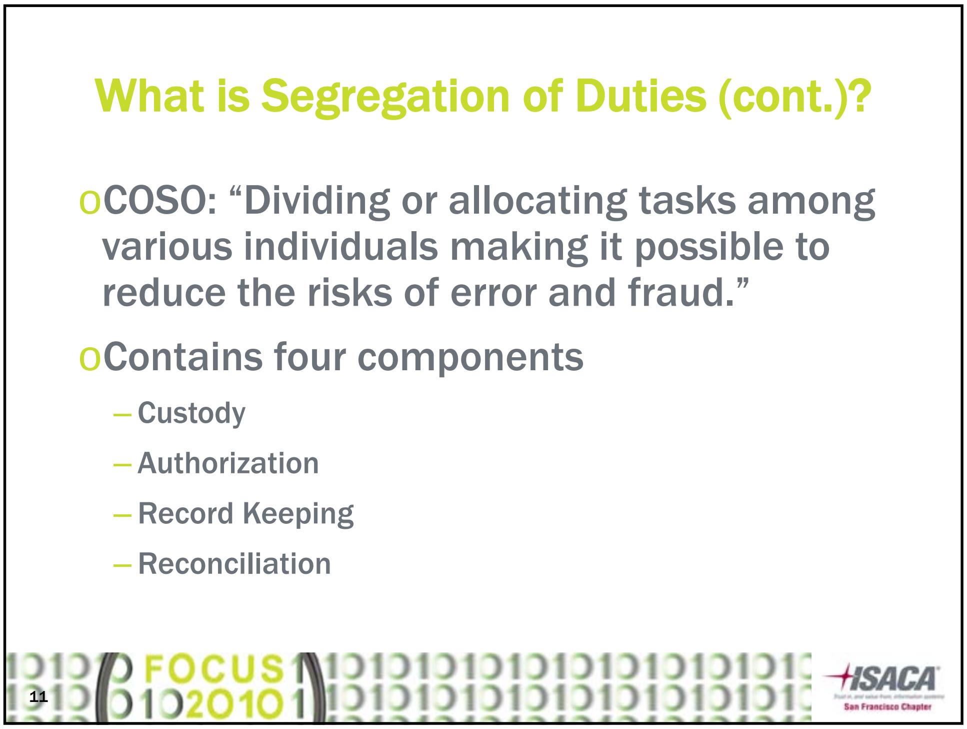
8

Management is Surprised…

- 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 vacation accruals and approve payment in-lieu of vacation

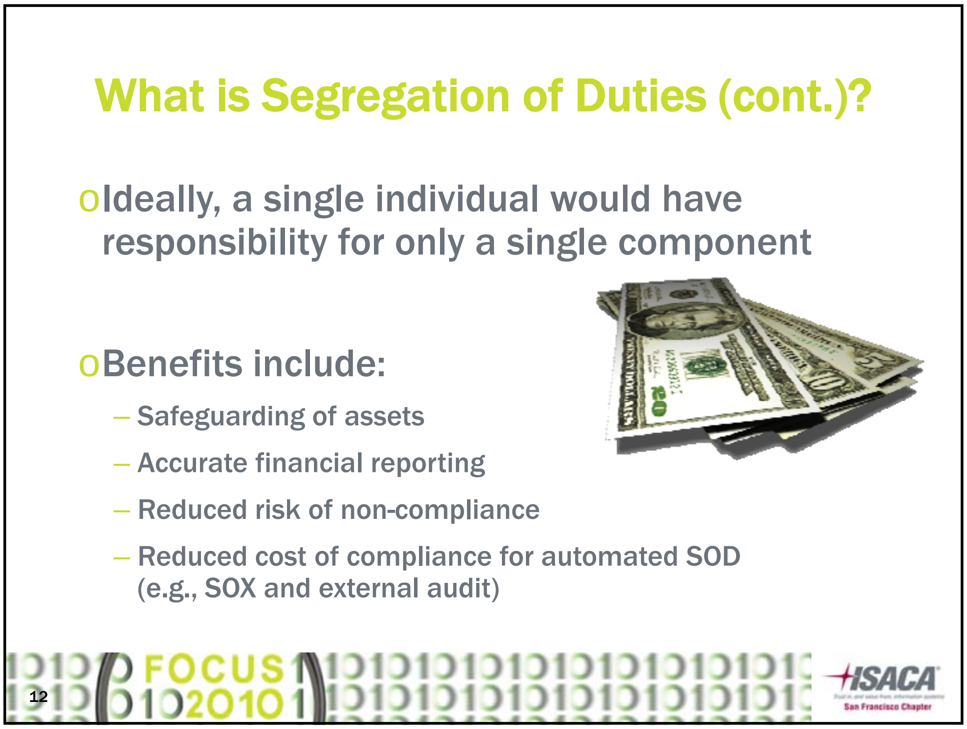
What is Segregation of Duties?

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



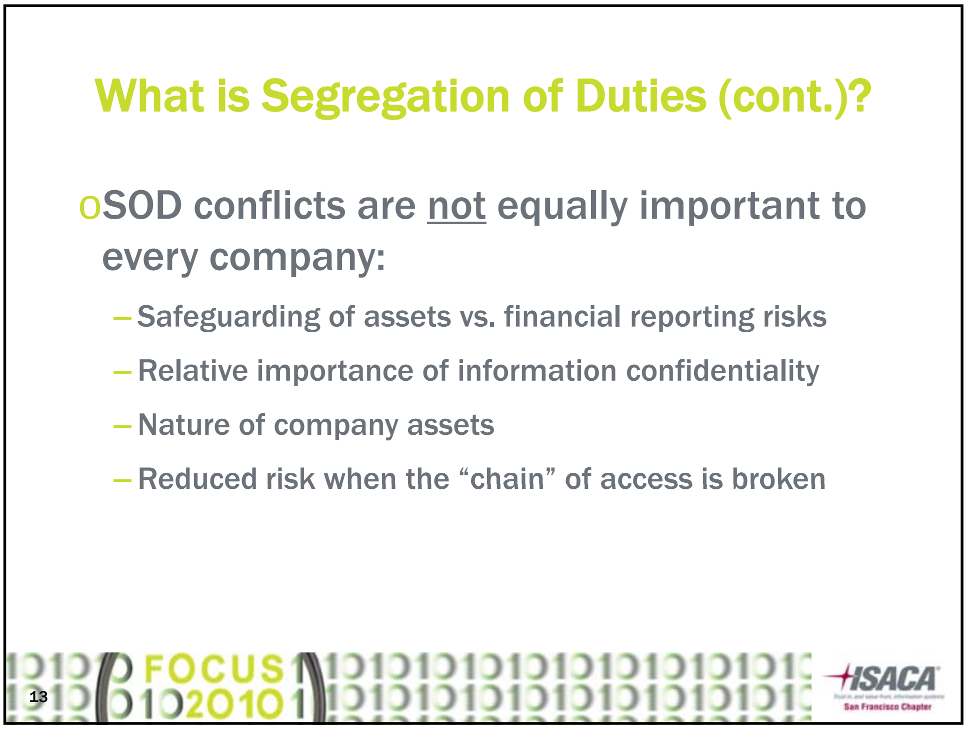
What is Segregation of Duties (cont.)?

- 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



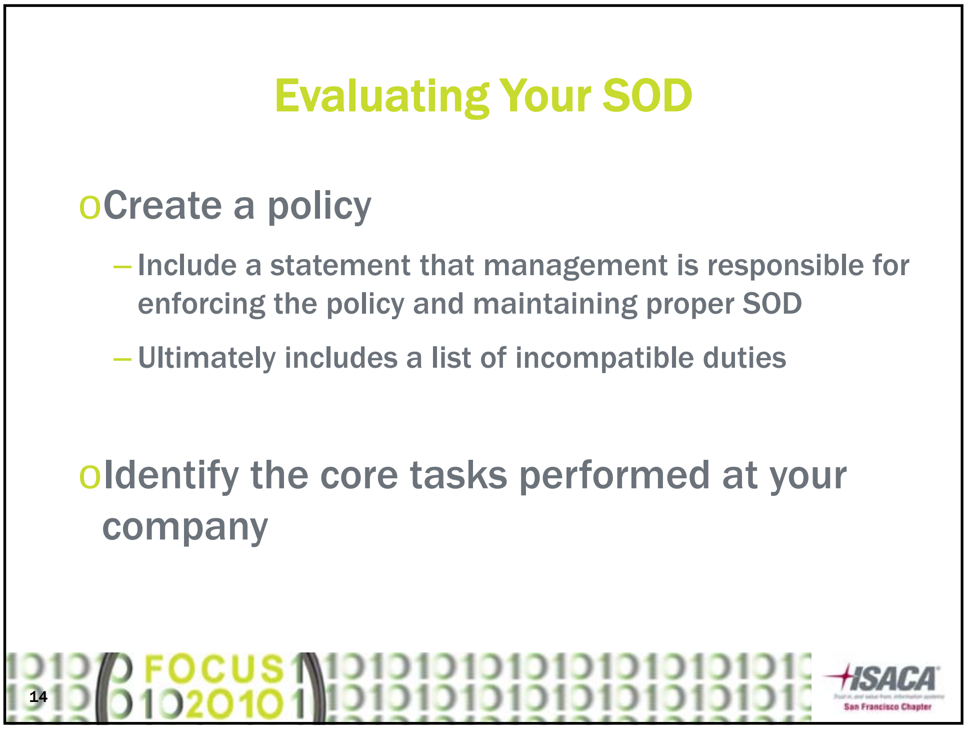
What is Segregation of Duties (cont.)?

- 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



Evaluating Your SOD

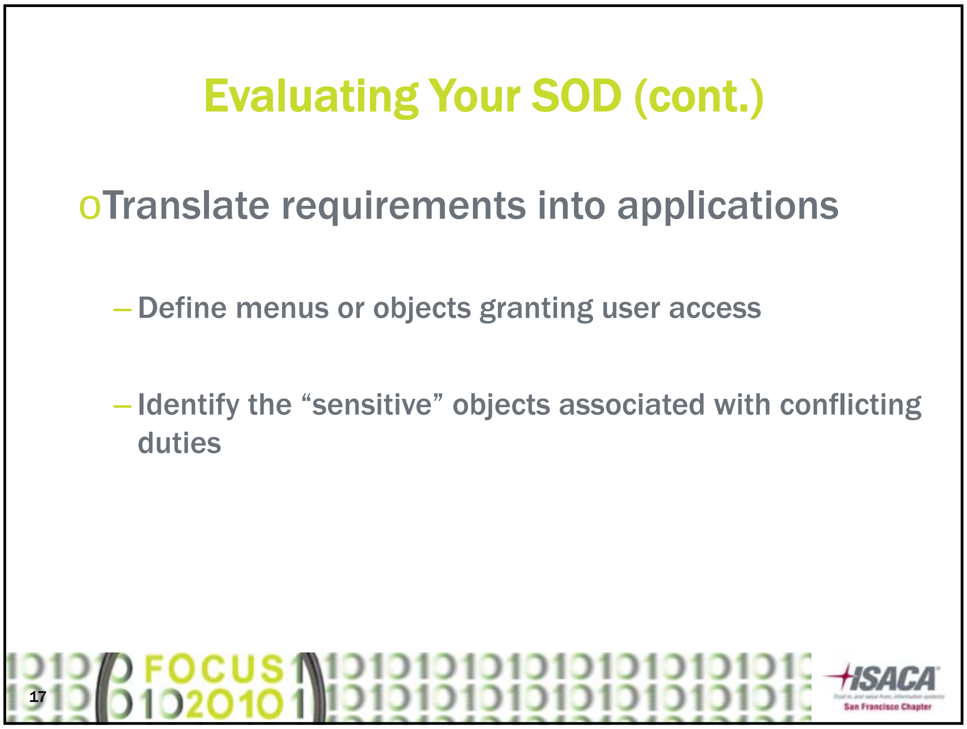
- Create a policy
  - Include a statement that management is responsible for enforcing the policy and maintaining proper SOD
  - Ultimately includes a list of incompatible duties
- Identify the core tasks performed at your company

Evaluating Your SOD

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

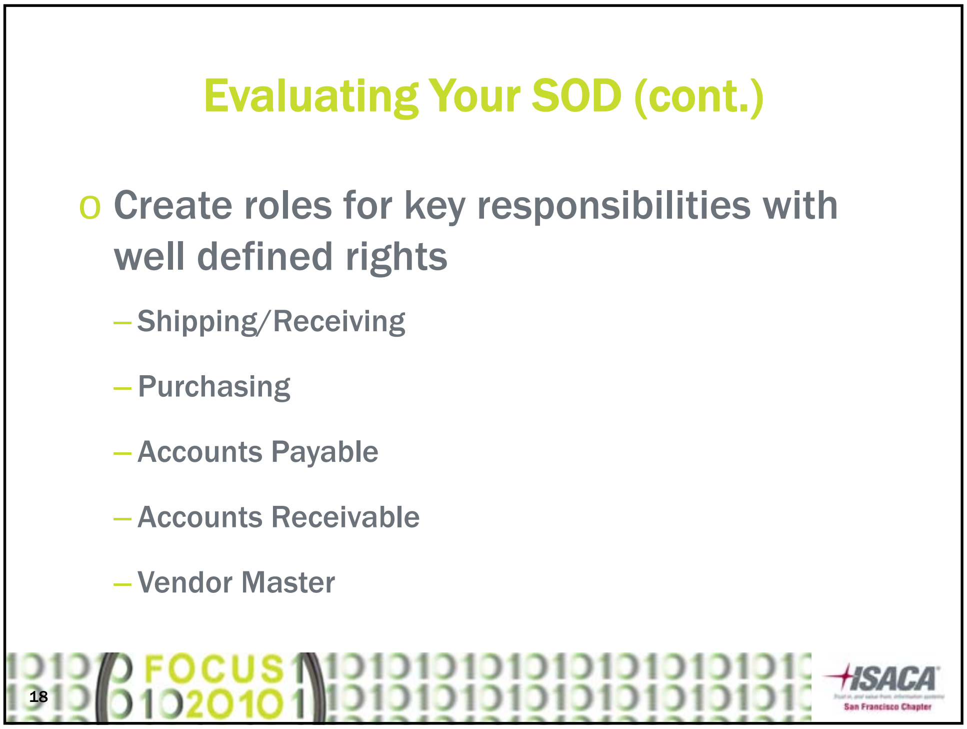
Example SOD Matrix

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.)

- Translate requirements into applications
  - Define menus or objects granting user access
  - Identify the “sensitive” objects associated with conflicting duties



Evaluating Your SOD (cont.)

- Create roles for key responsibilities with well defined rights
  - Shipping/Receiving
  - Purchasing
  - Accounts Payable
  - Accounts Receivable
  - Vendor Master

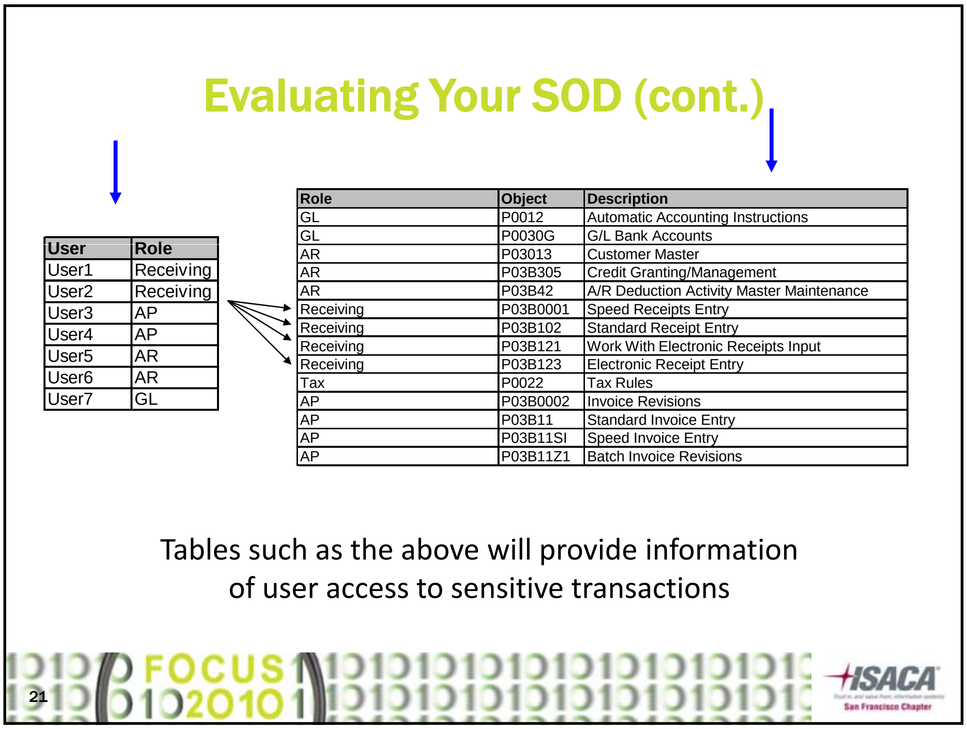
Evaluating Your SOD (cont.)

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
  - Provides a complete list of user conflicts allowed

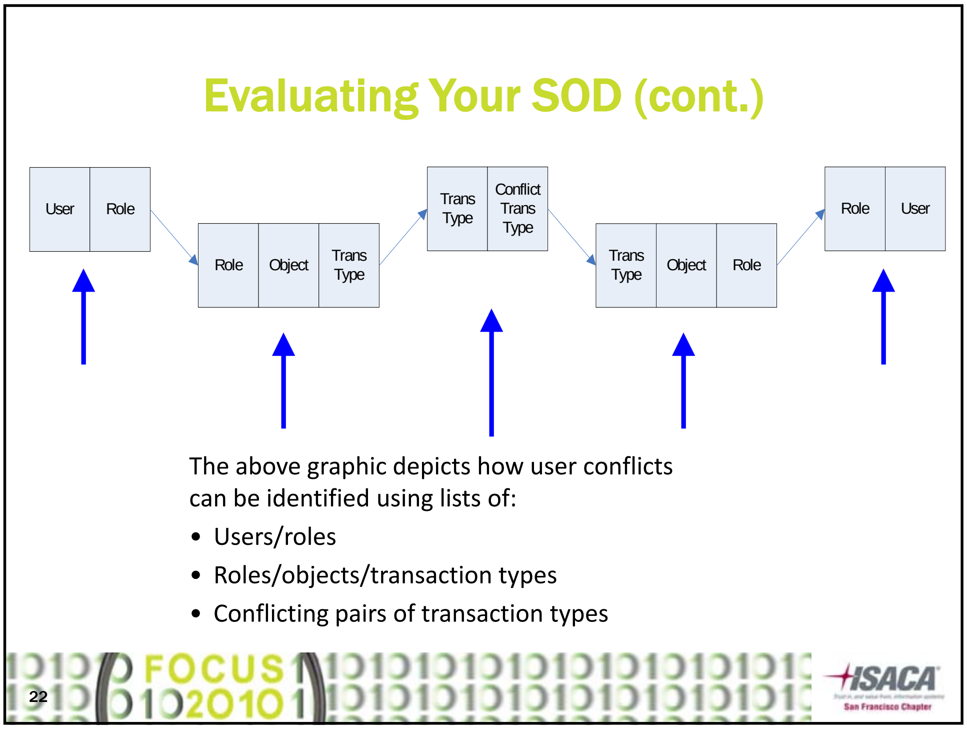


Evaluating Your SOD (cont.)

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:

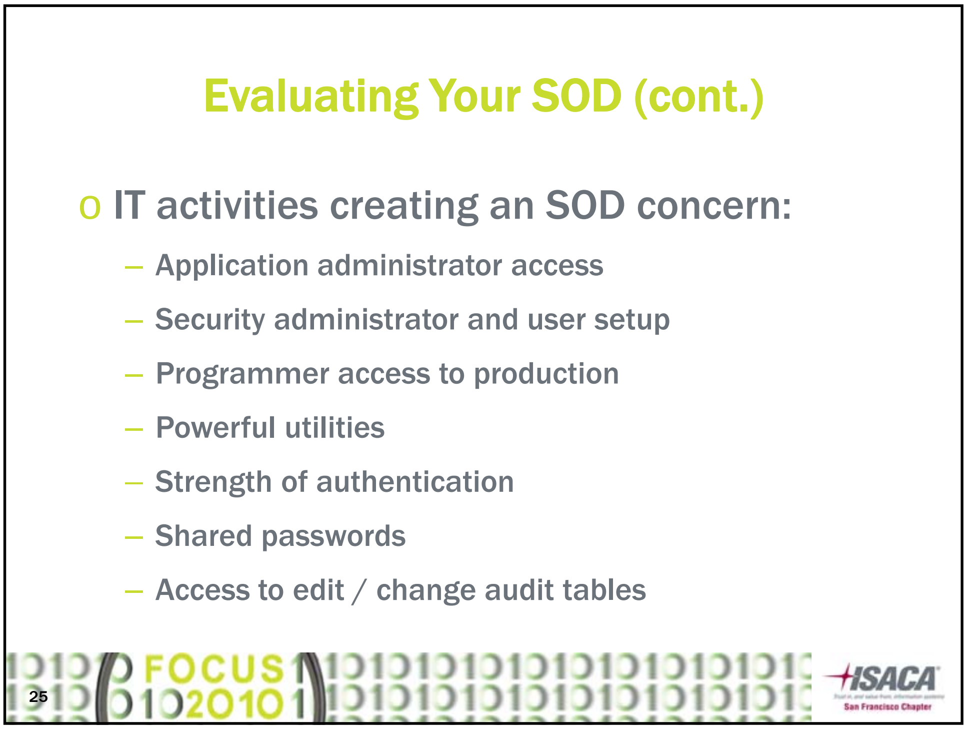
- Users/roles
- Roles/objects/transaction types
- Conflicting pairs of transaction types

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

Evaluating Your SOD (cont.)

- 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

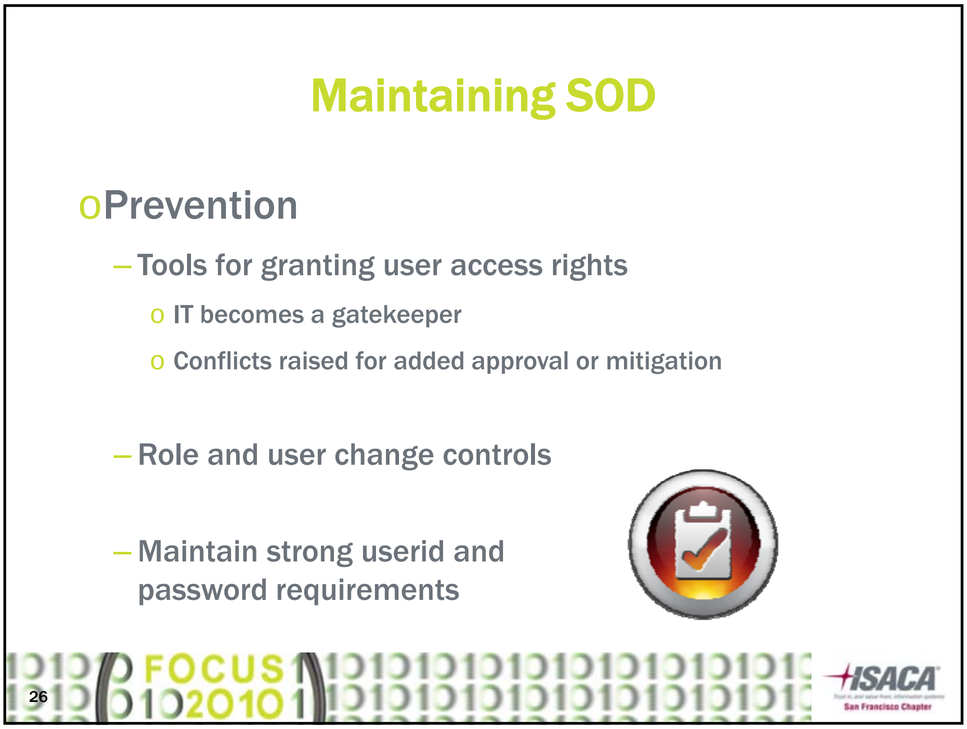


Evaluating Your SOD (cont.)

- 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

FOCUS 2010

ISACA San Francisco Chapter

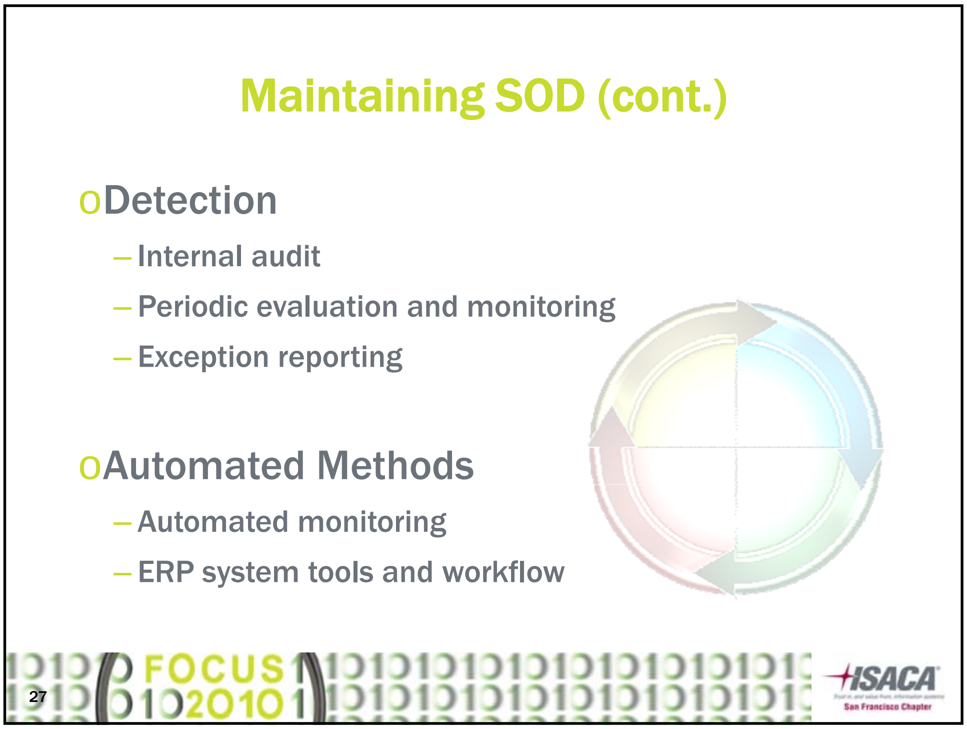


Maintaining SOD

- Prevention
  - Tools for granting user access rights
    - IT becomes a gatekeeper
    - Conflicts raised for added approval or mitigation
  - Role and user change controls
  - Maintain strong userid and password requirements

FOCUS 2010

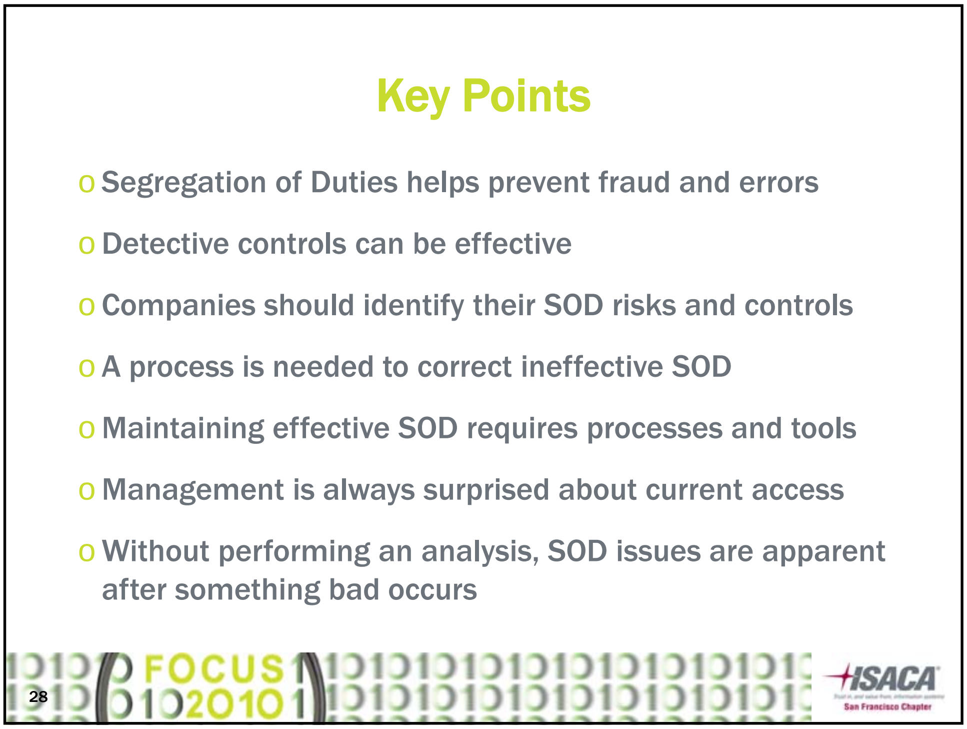
ISACA San Francisco Chapter



Maintaining SOD (cont.)

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

27



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
- Management is always surprised about current access
- Without performing an analysis, SOD issues are apparent after something bad occurs

28

Questions and Answers

Thank You For Attending

- Feel free to contact us
  - Eric Miles
    - Eric.Miles@mossadams.com
    - Office: (408) 916-0606
  - Scott Mitchell
    - Scott.Mitchell@mossadams.com
    - Office: (503) 478-2193