# A Risk-Based Approach to Segregation of Duties

## ISACA Charlotte SoD Discussion

28 October 2011

Ernst & Young

*Quality In Everything We Do*

# Introductions

## Justin Greis

Senior Manager
Advisory Practice
Chicago, Illinois

- BS ‘03, MBA ‘04 (Accounting/IS)
- CISSP, CISA, CISM, CGEIT, ITIL CIPP, GIAC/GSEC, PMP, CRISC, TOGAF *(in progress)*
- Professor of Information Systems at Indiana University, Bloomington, Kelley School of Business
- Specializations
  - IT Strategy & Effectiveness
  - Segregation of Duties
  - Identity & Access Management
  - Program & Project Management

## Chris Hansen

Manager
Advisory Practice
New York, New York

- BS ’04 (Information Systems)
- CISA, CISM, PMP, ISO 20000, ITIL v2, Six Sigma Green Belt
- Frequent speaker and guest lecturer at Indiana University, Kelley School of Business
- Focus on financial services industry
- Specializations
  - Program Management
  - Post Implementation Review
  - Risk and Compliance Audit
  - Trade Order Management

# What is Segregation of Duties (SoD)?

- Segregation of Duties (SoD) is a key internal control that, at the most basic level, attempts to ensure that no single individual should have control over two or more conflicting sensitive transactions
- SoD is not a new control; it has become more complicated as processes are automated and transactions are distributed throughout the organization

**Example**

A user with vendor update privileges should not have the ability to issue payments.

*Why?* The risk is that a user could add a fictitious vendor (i.e. the employee) and issue payments to that vendor.

# Why Does SoD Matter?

- Segregation of Duties (SoD) has become one of the most common control deficiencies in integrated audits
- SoD is difficult to test, correct and identify ownership
- Often the deficiency is given to IT since they are the “gate keepers” of access to the sensitive transactions in the computer systems
- IT will typically turn to Finance or Accounting groups to define the appropriate access levels to support the business processes

**Key Questions**

Who owns SoD in the organization?
How is SoD tested and maintained?
How are SoD conflicts mitigated and remediated?
What is the role of internal audit in achieving SoD compliance?

# Session Objectives

1. Understand SoD terminology, its impact on the organization and how to define SoD risk thresholds
2. Review the risk-based approach and critical success factors for testing SoD, regardless of application or platform
3. Introduce SoD mitigation and remediation techniques
4. Discuss internal audit's role in SoD compliance
5. Discuss how companies can effectively work together and work with external audit to achieve compliance

# Agenda

| Topic | Issue |
|---|---|

1. Background ..... *Understanding the Risk*

2. SoD Methodology & Approach
   - Business Definition ..... *Defining the Risk*
   - Technical Definition ..... *Mapping the Systems to the Risk*
   - Testing ..... *Measuring the Risk*
   - Mitigation ..... *Gaining Control*
   - Remediation ..... *Fixing the Issue*

3. Lessons Learned ..... *Avoiding Mistakes*

A Risk-Based Approach to Segregation of Duties

# BACKGROUND

# Let’s do a little experiment…


## Justin’s $50 Mistake

# Here is our scenario…

Stored in a secure lock-box

Sitting out on a table.

Guarded by someone who will alert me when the money is stolen.

Guarded by someone who will ward off thieves and alert authorities.

Protected by a motion detector alarm designed to automatically alert me of a theft.

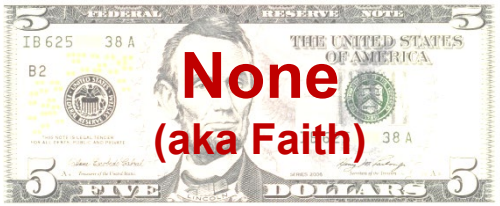
# Consider the following…

# Let’s Take a Walk

# Where's the Money?

# What controls were applied?


Stored in a secure lock-box



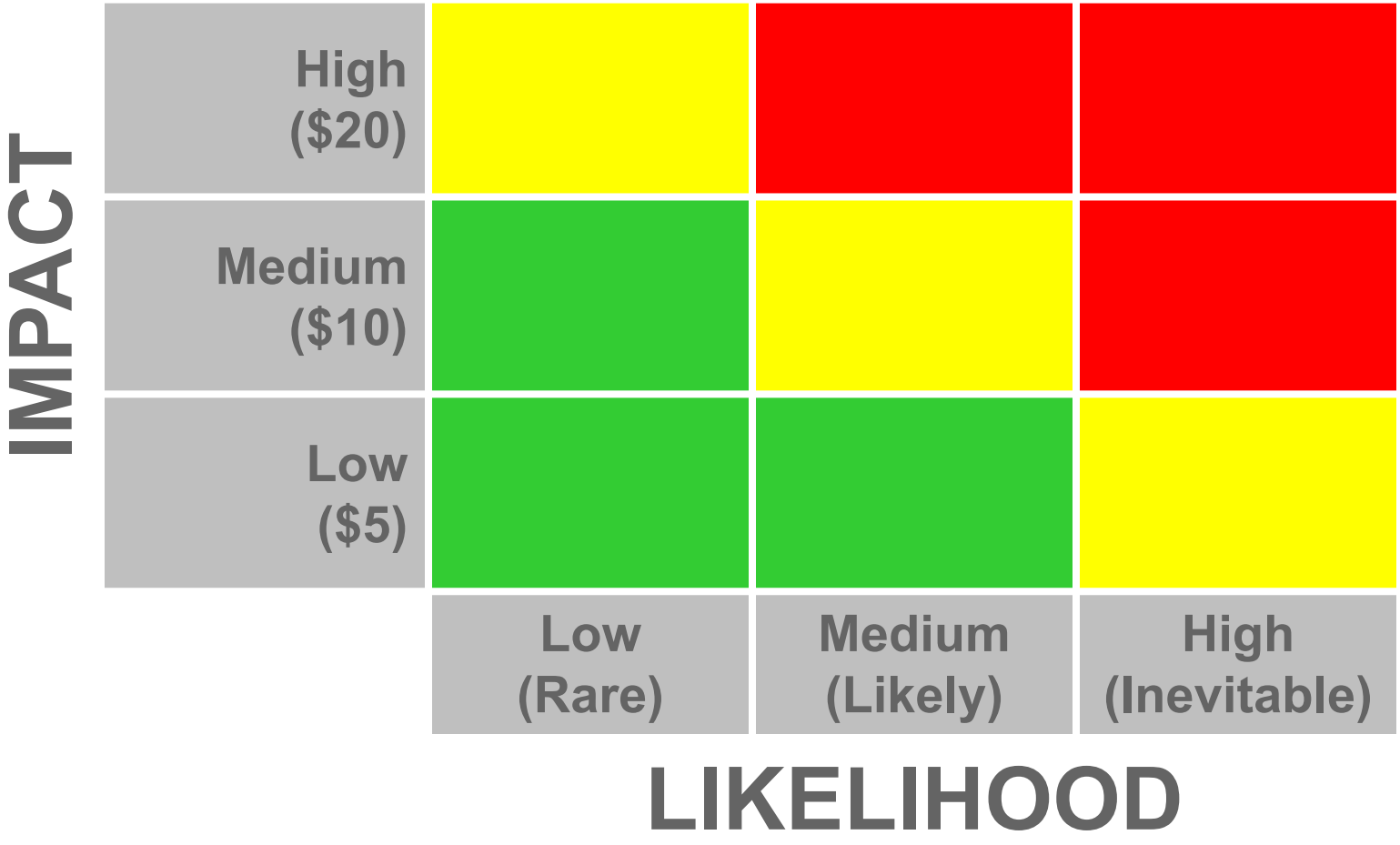

Sitting out on a table.


Guarded by someone who will alert me when the money is stolen.


Guarded by someone who will ward off thieves and alert authorities.


Protected by a motion detector alarm designed to automatically alert me of a theft.

# What is our risk profile?



# How can we apply governance to enhance the process?

- You are all a part of the **ISACA Charlotte Cash Council**. Our mission is to **protect the assets of the company**.

- In this meeting we must discuss:
  - **What** happened to my $50?!?!?!
  - **Why** did this happen…
  - **How** can we make this process better?

- Once you come up with your recommendations, implement it so we can test it out.

- Let's try the exercise again.

# Let's Take a Walk…

# Where's my money?

# Take away…

**A company's ability to protect its assets and mitigate the risk of fraud are only as good as the as its ability to work together to optimize its control environment.**

# SoD Terminology

- **Business Process** – The high-level mega processes in which transactions are executed (i.e. purchase-to-pay, order-to-cash, financial reporting, etc.)
- **Sensitive Transaction** – A business transaction that drives the associated processes with the potential to impact the financial statements
- **SoD Conflict** – The pairing of two conflicting sensitive transactions
- **SoD Conflict Matrix*** – The chart that shows the complete SoD conflicts (independent of application)
- **Materiality** – The financial threshold/impact a potential SoD conflict can have over the financial statements

* Also known as the “Mileage Chart”

# Drivers for Segregation of Duties

- Regulatory Compliance
  - SEC Guidance such as the recent cyber-security disclosure requirement
  - US Sarbanes-Oxley (SOX)/KSOX/JSOX
  - Gramm-Leach-Bliley Act (GLBA)
  - Health Insurance Portability and Accountability Act (HIPAA)
  - Federal Financial Institutions Examination Council (FFIEC)
  - BASEL II & Solvency II
  - EU's 8th Directive and other Global 'SOX-type' Laws
- Internal/External Financial Audit Compliance
- Risk/Fraud Mitigation
- Continuous Control Monitoring

**Important**

SoD is an *expectation* of investors, clients/customers and business partners alike. It is a critical fraud-prevention control.

# Impact of Material Weakness

CFO.com

**How Markets Punish Material Weaknesses**

**A new report examines shortcomings that lead to losses in share price; Sarbanes-Oxley requirements are understood poorly by investors, say some observers.**

Marie Leone, CFO.com
July 21, 2005

Section 404 of the Sarbanes-Oxley Act requires companies to disclose internal-control deficiencies in their annual reports. The effects on share prices are examined in "Control Deficiencies: Finding Financial Impurities," a new analysis of 2004 and early 2005 disclosures by shareholder-advisory firm Glass, Lewis & Co.

Glass Lewis examined companies with a market capitalization in excess of $75 million. About 11 percent of these companies disclosed a control deficiency between January 1, 2004, and May 2, 2005. The number of companies that disclosed a material weakness — the most severe control problem — totaled 586 for the first four months of 2005, compared with 313 for all of 2004, according to the report.

On average, the day after a company disclosed a material weakness in its financial controls, its share price dropped 0.67 percent relative to market movement, Glass Lewis found. After 7 days, the share price dropped 0.90 percent; after 30 days, 1.96 percent; and after 60 days, 4.06 percent. "The mere announcement of a material weakness, independent of the auditor opinion, appears to solicit a negative reaction from investors," according to the study.

Average Share Price Movement, Relative to Market, vs. Seven Days before Announcement

| | 1 day after | 7 days after | 30 days after | 60 days after |
|---|---|---|---|---|
| All Deficiencies | -0.72% | -0.81% | -1.50% | -3.02% |
| Material Weaknesses | -0.67% | -0.90% | -1.96% | -4.06% |
| Qualified Opinions | -0.23% | -0.66% | -2.30% | -3.56% |
| Qualified Opinions, No Warning | -0.04% | -0.16% | -2.49% | -3.94% |

Sources: Glass Lewis, FactSet.

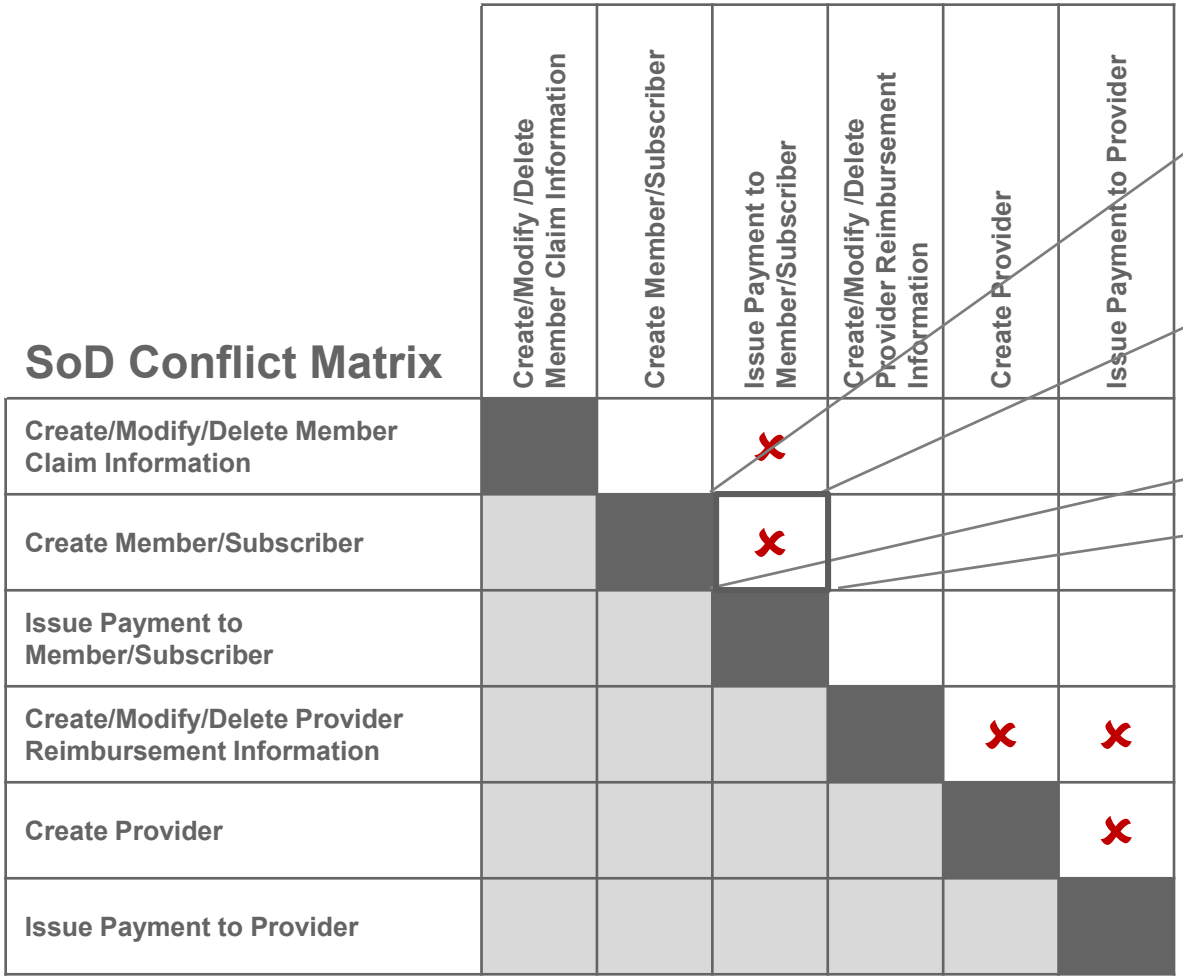
**-4.06%**

Source: http://www.cfo.com/article.cfm/4197475?f=search

# Common SoD Observations

| Observation | Description |
|---|---|
| **Testing overkill** | Too many defined conflicts make SoD controls and sustained compliance difficult and onerous on the business. |
| **Testing inadequacy** | Insufficient or undefined SoD conflicts or SoD testing methodology. This may represent a failure to capture the high risk conflicts. |
| **Improper SoD reporting** | Reporting conflict counts and risks is inconsistent – can be overstated or understated depending on aggregation approach. |
| **Complex systems and application suites** | Multiple systems make cross-application testing complex. Some legacy systems are not capable of achieving adequate SoD. |
| **Inadequate tools for ongoing compliance** | Testing and compliance tools enable sustained compliance and on-demand testing. |
| **Unclear SoD governance** | Technology is often given the deficiency, but business is responsible for determining the risk. |
| **Inconsistent User ID conventions** | With so many applications, it is often difficult to determine who has access to what based on consistent user IDs. |
| **Lack of mitigation strategy** | Existing controls can be leveraged to compensate for the risk of existing conflicts, but need a framework to achieve compliance |
| **Fragmented remediation initiatives** | IT can enable ongoing compliance through Identity & Access Management (IAM) tools and processes rather than one-off solutions |

# Illustrative High Level Healthcare SoD Conflict Matrix




**Risk Statement**

*A user could create fictitious members/ subscribers and issue unauthorized/ fraudulent payments to those members/ subscribers.*

**Key Considerations**

- How many users meet this condition?
- What mitigating controls are in place?
- How do we detect and prevent this risk from occurring?

# A Note on IT Segregation of Duties

- IT SoD and privileged access control is typically addressed through IT General Controls
  - Logical Access
  - Change Management
  - Operations
- Example controls employed to mitigate IT SoD risks:
  - Staged development application environments (e.g. development, test, QA, production, etc.)
  - Break-glass/emergency check-out procedures
  - Password vault and password checkout alerting
  - Monitoring and logging of privileged accounts
  - Periodic review and recertification of privileged accounts
  - Restricted access based on roles (see corresponding exhibit)
  - Business reconciliation controls

**Example IT Segregation of Duties Matrix**

| | Control Group | Systems Analyst | Application Programmer | Help Desk and Support Manager | End User | Data Entry | Computer Operator | Database Administrator | Network Administrator | Systems Administrator | Security Administrator | Systems Programmer | Quality Assurance |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Control Group | | X | X | X | | X | X | X | X | X | | X | |
| | | | | X | X | | X | | | | X | | X |
| | | | X | X | X | X | X | X | X | X | X | X | X |
| | | X | | X | X | | X | X | X | X | | X | |
| | | X | X | | | | X | X | X | | | X | X |
| | | X | X | | | X | | X | X | X | X | X | |
| | | X | X | X | X | X | X | | X | X | | X | |
| Network Administrator | X | | X | X | X | X | X | X | | | | | |
| System Administrator | X | | X | X | | X | X | X | | | | X | |
| Security Administrator | | X | X | | | X | X | | | | | X | |
| Systems Programmer | X | | X | X | X | X | X | X | | X | X | | X |
| Quality Assurance | | X | X | | X | | | | | | | X | |

X—Combination of these functions may create a potential control weakness.

Source: ISACA

**Risk Statement**

*A programmer could create a privileged account, make a change to the business logic of an application and mask the activity by deleting the accounts and logs.*

**Note:** The conflict matrix above illustrates potential segregation of duties conflicts that can occur within the technology organization. A similar approach is used to test for these conflicts, but a different set of controls are applied to mitigate the IT risks of privileged and super users.

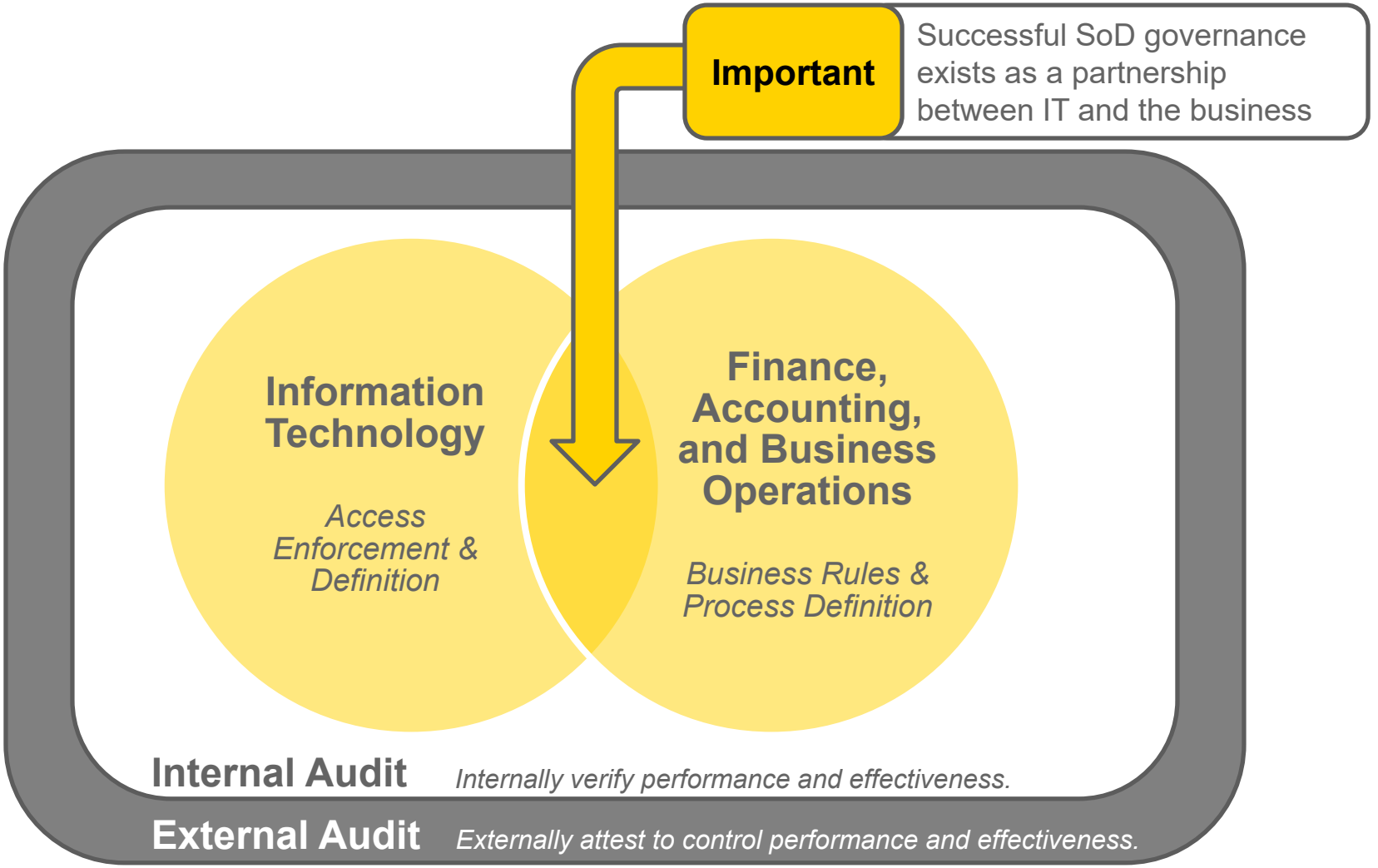
# Stakeholders

- **CFO & CIO** – Leadership must support business process reengineering and/or changes to control structure in order to remediate/mitigate SoD control failures
- **Internal Audit/Compliance** – Internal audit/compliance can assist with testing and mitigating control documentation
- **Business Finance Personnel** – Finance personnel have knowledge of the sensitive transactions and business processes creating the SoD conflicts
- **IT Personnel** – IT personnel have the knowledge of the applications that enable the execution of the sensitive transactions
- **External Audit Parties** – External audit must ultimately attest to the effectiveness of the internal control environment

**Note**

Stakeholders can change with each company and/or business unit. Successful SoD programs depend on the involvement of *both* IT and Finance personnel.

# SoD Ownership & Governance



A Risk-Based Approach to Segregation of Duties

# SOD METHODOLOGY & APPROACH

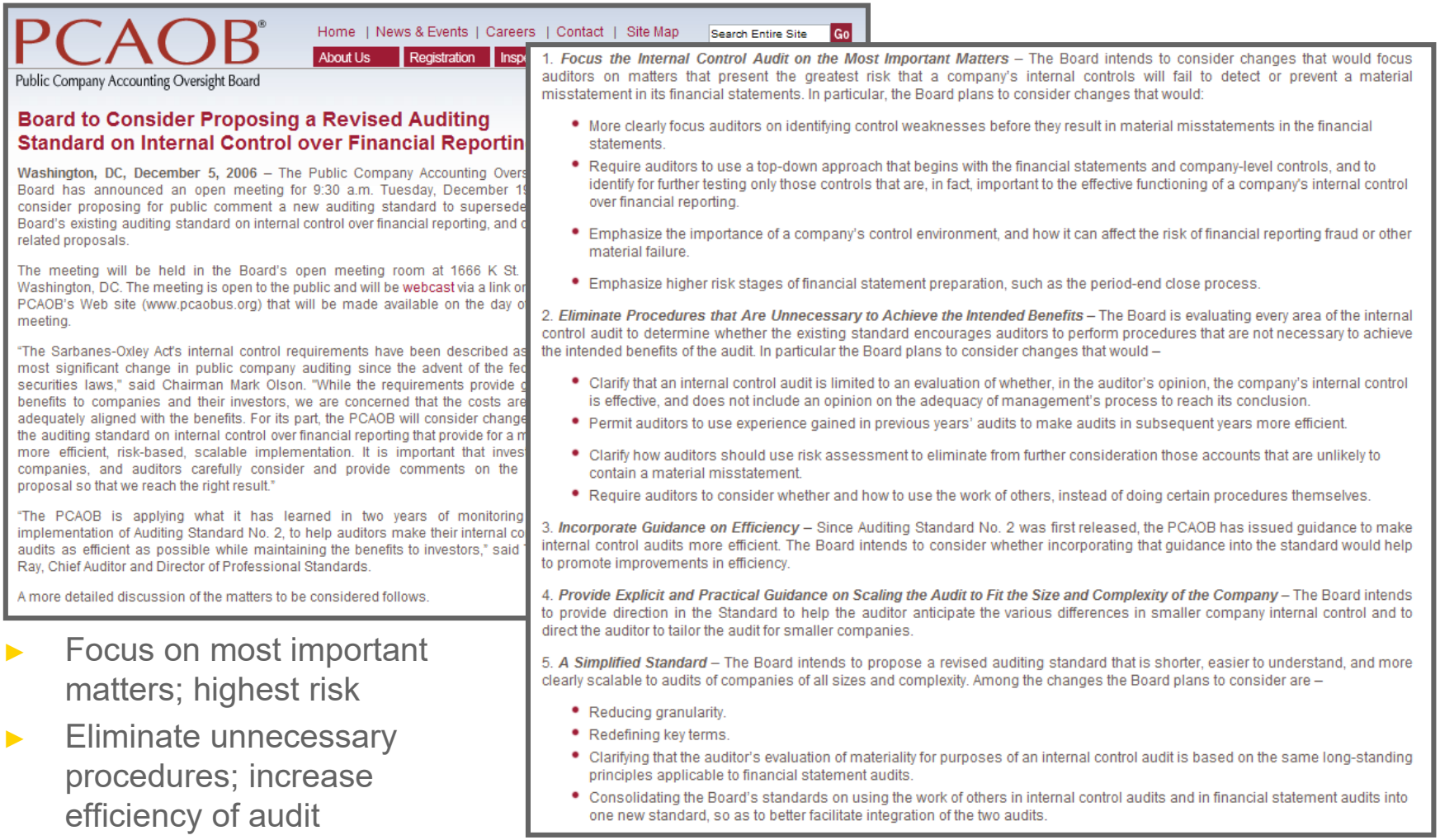
# Why Risk-Based?

- Focuses time on transactions that pose the greatest risk the organization
- Risk levels can be tuned to achieve SoD program objectives (detect fraud, detect material impact to financial statements, enforce monitoring controls, etc.)
- Focuses testing and remediation efforts of limited resources
- Satisfies compliance and regulatory objectives
- “Don’t try to boil the ocean”

**What is Risk-Based?**

Risk-based refers to targeting the processes, transactions, and conflicts that present the greatest threat of fraud, wrong-doing or material misstatement to the business.

# PCAOB Auditing Standard No. 5



PCAOB®

Public Company Accounting Oversight Board

Home | News & Events | Careers | Contact | Site Map

Search Entire Site Go

About Us | Registration | Insp

**Board to Consider Proposing a Revised Auditing Standard on Internal Control over Financial Reportin**

**Washington, DC, December 5, 2006** – The Public Company Accounting Overs Board has announced an open meeting for 9:30 a.m. Tuesday, December 1 consider proposing for public comment a new auditing standard to supersede Board's existing auditing standard on internal control over financial reporting, and c related proposals.

The meeting will be held in the Board's open meeting room at 1666 K St. Washington, DC. The meeting is open to the public and will be webcast via a link or PCAOB's Web site (www.pcaobus.org) that will be made available on the day o meeting.

"The Sarbanes-Oxley Act's internal control requirements have been described as most significant change in public company auditing since the advent of the fed securities laws," said Chairman Mark Olson. "While the requirements provide g benefits to companies and their investors, we are concerned that the costs are adequately aligned with the benefits. For its part, the PCAOB will consider change the auditing standard on internal control over financial reporting that provide for a m more efficient, risk-based, scalable implementation. It is important that inves companies, and auditors carefully consider and provide comments on the proposal so that we reach the right result."

"The PCAOB is applying what it has learned in two years of monitoring implementation of Auditing Standard No. 2, to help auditors make their internal co audits as efficient as possible while maintaining the benefits to investors," said Ray, Chief Auditor and Director of Professional Standards.

A more detailed discussion of the matters to be considered follows.

1. ***Focus the Internal Control Audit on the Most Important Matters*** – The Board intends to consider changes that would focus auditors on matters that present the greatest risk that a company's internal controls will fail to detect or prevent a material misstatement in its financial statements. In particular, the Board plans to consider changes that would:

- More clearly focus auditors on identifying control weaknesses before they result in material misstatements in the financial statements.
- Require auditors to use a top-down approach that begins with the financial statements and company-level controls, and to identify for further testing only those controls that are, in fact, important to the effective functioning of a company's internal control over financial reporting.
- Emphasize the importance of a company's control environment, and how it can affect the risk of financial reporting fraud or other material failure.
- Emphasize higher risk stages of financial statement preparation, such as the period-end close process.

2. ***Eliminate Procedures that Are Unnecessary to Achieve the Intended Benefits*** – The Board is evaluating every area of the internal control audit to determine whether the existing standard encourages auditors to perform procedures that are not necessary to achieve the intended benefits of the audit. In particular the Board plans to consider changes that would –

- Clarify that an internal control audit is limited to an evaluation of whether, in the auditor's opinion, the company's internal control is effective, and does not include an opinion on the adequacy of management's process to reach its conclusion.
- Permit auditors to use experience gained in previous years' audits to make audits in subsequent years more efficient.
- Clarify how auditors should use risk assessment to eliminate from further consideration those accounts that are unlikely to contain a material misstatement.
- Require auditors to consider whether and how to use the work of others, instead of doing certain procedures themselves.

3. ***Incorporate Guidance on Efficiency*** – Since Auditing Standard No. 2 was first released, the PCAOB has issued guidance to make internal control audits more efficient. The Board intends to consider whether incorporating that guidance into the standard would help to promote improvements in efficiency.

4. ***Provide Explicit and Practical Guidance on Scaling the Audit to Fit the Size and Complexity of the Company*** – The Board intends to provide direction in the Standard to help the auditor anticipate the various differences in smaller company internal control and to direct the auditor to tailor the audit for smaller companies.

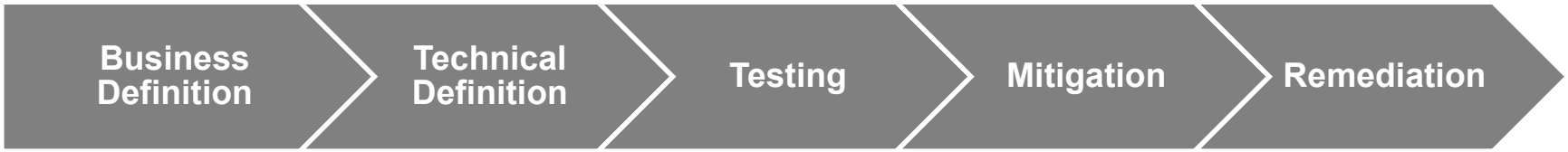
5. ***A Simplified Standard*** – The Board intends to propose a revised auditing standard that is shorter, easier to understand, and more clearly scalable to audits of companies of all sizes and complexity. Among the changes the Board plans to consider are –

- Reducing granularity.
- Redefining key terms.
- Clarifying that the auditor's evaluation of materiality for purposes of an internal control audit is based on the same long-standing principles applicable to financial statement audits.
- Consolidating the Board's standards on using the work of others in internal control audits and in financial statement audits into one new standard, so as to better facilitate integration of the two audits.

- Focus on most important matters; highest risk
- Eliminate unnecessary procedures; increase efficiency of audit

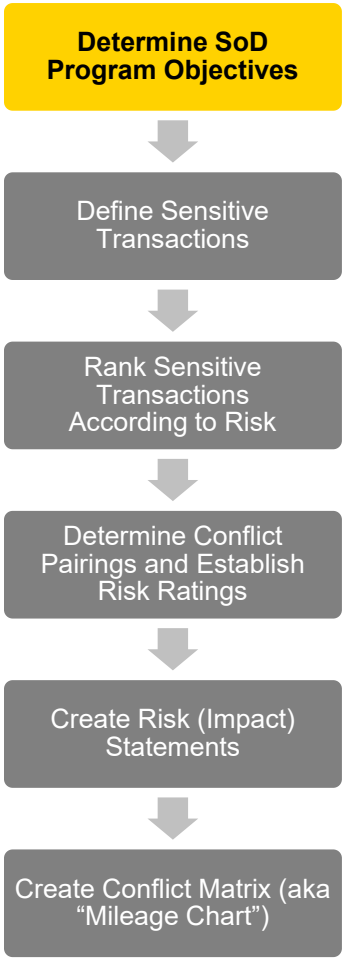
Source: http://www.pcaob.org/News_and_Events/News/2006/12-05.aspx

# SoD Phases




- **Business Definition**
  - Defines the scope of sensitive transactions and conflicts – based on risk – that drive a company's key business processes
- **Technical Definition**
  - Maps the defined sensitive transactions to system and application capabilities
- **Testing**
  - Analyzes the user entitlements to provide a current state view of the SoD conflicts
- **Mitigation**
  - Cites valid, effective financial controls that mitigate the risk for existing and/or potential conflicts
- **Remediation**
  - Corrects the issues noted in testing using various methods such as role redesign, tactical user cleanup, identity & access management, and appropriate user access reviews

# Determine Program Objectives




- SoD program objectives determine the overall level of risk that management is willing to accept
- Results in the establishment of a program mission statement and/or overall control target

**Example 1** The objective of this SoD initiative is to prevent or detect potential fraudulent or unauthorized transactions that meet the level of materiality.

**Example 2** The objective of this SoD initiative is to detect excessive access within the financial reporting and purchase-to-pay processes.

**Example 3** The objective of this SoD initiative is to detect fraudulent transactions in excess of $1,000.

**Business Definition** | **Technical Definition** | **Testing** | **Mitigation** | **Remediation**

# Define Sensitive Transactions

Determine SoD Program Objectives

**Define Sensitive Transactions**

Rank Sensitive Transactions According to Risk

Determine Conflict Pairings and Establish Risk Ratings

Create Risk (Impact) Statements

Create Conflict Matrix (aka "Mileage Chart")

- Sensitive transactions are compiled based on the processes that drive the business
- Sensitive transactions are gathered through:
  - Workshops, interviews, observation of business processes, walkthrough, audit documentation, etc.

| SoD Group | Business Process | Sensitive Transactions |
|---|---|---|
| 1 | Sales & Receivables | Create/Modify/Delete Customer Pricing Master/Structure |
| 2 | Sales & Receivables | Create/Modify/Delete Manual Sales Invoices/Manual Service Invoices |
| 3 | Sales & Receivables | Create/Modify/Delete Customer Credit Memos |
| 4 | Sales & Receivables | Post Cash Receipts & Apply to Customer Account |
| 5 | Sales & Receivables | Create/Modify/Delete Customer Master Data |
| 6 | Sales & Receivables | Create/Modify/Delete Sales Orders/Service Orders |
| 7 | Sales & Receivables | Create/Modify/Delete Customer Credit Limits |
| 8 | Purchasing | Create/Modify/Delete Purchase Orders |
| 9 | Purchasing | Create/Modify/Delete Vendor Master File Data |
| 10 | Purchasing | Approve Purchase Orders |
| 11 | Inventory Master Data | Create/Change Standard or Actual Costing |
| 12 | Inventory Master Data | Create/Change to Material Master Data |
| 13 | Inventory Transactions | Record Inventory Movements or Production |
| 14 | Inventory Transactions | Record/Modify Shipment |
| 15 | Inventory Transactions | Receive/Post Physical Inventory or Cycle Counts |
| 16 | Fixed Assets | Create/Modify/Delete Fixed Asset Records (Additions) |
| 17 | Fixed Assets | Disposal/Retirement of Fixed Assets |
| 18 | Fixed Assets | Depreciation of Fixed Assets |
| 19 | Accounts Payable | Post PO & Non PO Invoices |
| 20 | Accounts Payable | Release on-hold Invoices |
| 21 | Accounts Payable | Post Goods Receipt (Services & Inventory) |
| 22 | Accounts Payable | Invoice Payment Run (Cash Disbursements) |
| 23 | | ords |
| 24 | | cords |
| 25 | | |

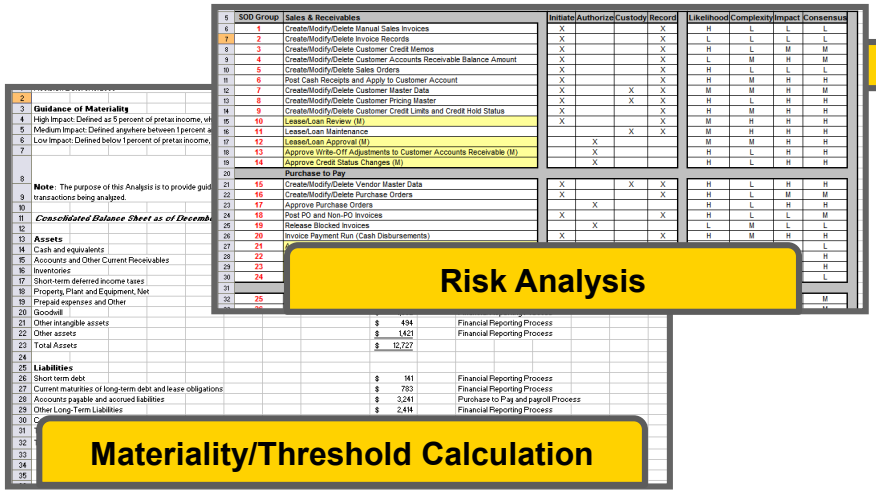
**Sensitive Transaction Listing**

**Business Definition** | Technical Definition | Testing | Mitigation | Remediation

# Rank Sensitive Transactions According to Risk

- Determine SoD Program Objectives
- Define Sensitive Transactions
- **Rank Sensitive Transactions According to Risk**
- Determine Conflict Pairings and Establish Risk Ratings
- Create Risk (Impact) Statements
- Create Conflict Matrix (aka "Mileage Chart")

- Establishes scope of sensitive transaction to be tested
- Risk analysis of transactions factors: likelihood, complexity, impact and arrives at a final consensus
- Transactions analyzed based on: materiality calculation, type of transaction, initiation, authorization, custody of assets, and recording of assets



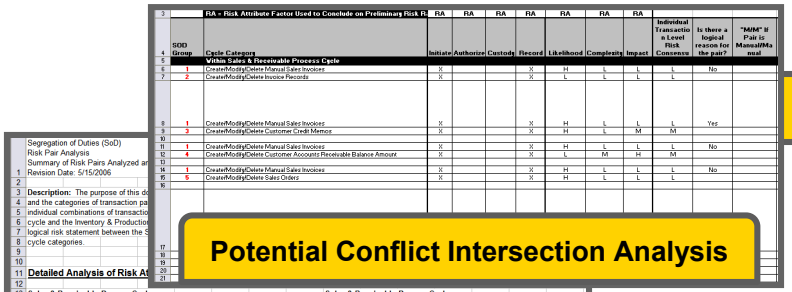

- Transaction 1
- Transaction 2
- Transaction 3
- Transaction 4

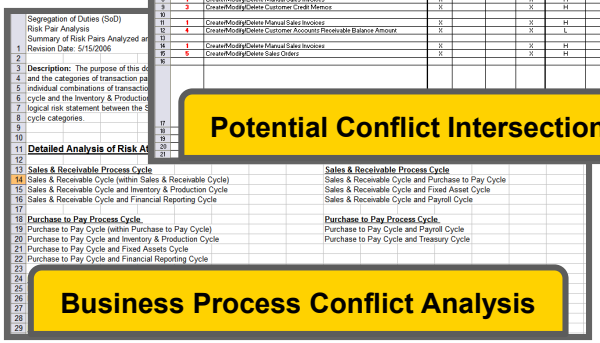
**Business Definition** → Technical Definition → Testing → Mitigation → Remediation

# Determine Conflict Pairings and Establish Risk Ratings

- Determine SoD Program Objectives
- Define Sensitive Transactions
- Rank Sensitive Transactions According to Risk
- **Determine Conflict Pairings and Establish Risk Ratings**
- Create Risk (Impact) Statements
- Create Conflict Matrix (aka "Mileage Chart")

- Conflict pairings are determined by examining the risk of combining each business process and every sensitive transaction
- Risk analysis is performed on each potential sensitive transaction to justify any potential omissions from testing




Transaction 1 + Transaction 2

Transaction 1 + Transaction 3

Transaction 1 + Transaction 4

**Business Definition** → Technical Definition → Testing → Mitigation → Remediation

# Determine Conflict Pairings and Establish Risk Ratings (Cont.)


- Once individual transactions are established and ranked, conflict pairings are created
- Not all SoD conflicts are created equally; some pose a greater risk and require special treatment
- Business stakeholders rank the conflicts parings according to the likelihood and impact of potential fraud

| | | | | |
|---|---|---|---|---|
| Transaction 1 | + | Transaction 2 | = | Risk |
| Transaction 1 | + | Transaction 3 | = | Risk |
| Transaction 1 | + | Transaction 4 | = | Risk |

**Risk Legend**

| | |
|---|---|
| High | Conflict not permitted |
| Medium | Conflict permitted with adequate mitigating controls and controller/VP/executive approval |
| Low | Conflict permitted with adequate mitigating controls and business process owner/director approval |

**Business Definition** → Technical Definition → Testing → Mitigation → Remediation

# Create Risk Statements

- Determine SoD Program Objectives
- Define Sensitive Transactions
- Rank Sensitive Transactions According to Risk
- Determine Conflict Pairings and Establish Risk Ratings
- **Create Risk (Impact) Statements**
- Create Conflict Matrix (aka "Mileage Chart")

- Risk statements are created for each potential SoD conflict pairing
- These statements convey the "impact" or the "what could go wrong" should a user have access to both conflicting sensitive transactions

**Create/Modify/Delete Customer Pricing Master/Structure** + **Create/Modify/Delete Manual Sales/Service Invoices** = **Risk Statement**

| | SoD Sensitive Transaction Group 1 | | | SoD Sensitive Transaction Group 2 | | | |
|---|---|---|---|---|---|---|---|
| ID | Business Process 1 | SoD Group 1 | Sensitive Transaction 1 | Business Process 2 | SoD Group 2 | Sensitive Transaction 2 | Risk Statement |
| 1 | Sales & Receivables | 1 | Create/Modify/Delete Customer Pricing Master/Structure | Sales & Receivables | 2 | Create/Modify/Delete Manual Sales Invoices/Manual Service Invoices | A user could modify pricing terms and manipulate the customer's sales invoice to offer favorable payment terms to the customer. |
| 2 | Sales & Receivables | 1 | Create/Modify/Delete Customer Pricing Master/Structure | Sales & Receivables | 3 | Create/Modify/Delete Customer Credit Memos | A user could modify the pricing condition on a customer's record and create a credit memo in favor of the customer for the price difference in a given order. |
| 3 | Sales & Receivables | 1 | Create/Modify/Delete Customer | Sales & Receivables | 4 | Post Cash Receipts & Apply to | A user could modify the pricing condition on a customer's record and apply an insufficient payment on a customer's account. |
| 4 | Sales & Receivabl | | | | | | A user could modify pricing terms and manipulate sales/service orders to offer favorable pricing for the customer. |
| 5 | Sales & Receivabl | | | | | | A user could modify shipping terms in the customer pricing master and modify shipping terms on shipping documents to record revenue in an incorrect period. |
| 6 | Sales & Receivabl | | Pricing Master/Structure | | | System | A fictitious user account could be created and granted access to conflicting functions, which enables them to perform unauthorized activities. This account could later be deleted, there by removing any traces of this malicious activity. |
| 7 | Sales & Receivables | 2 | Create/Modify/Delete M Sales Invoices/Manual Invoices | | | Modify/Delete Customer lemos | A user could enter a manual sales invoice and subsequently offset with a credit memo. |

A user could modify pricing terms and manipulate the customer's sales invoice to offer favorable payment terms to the customer

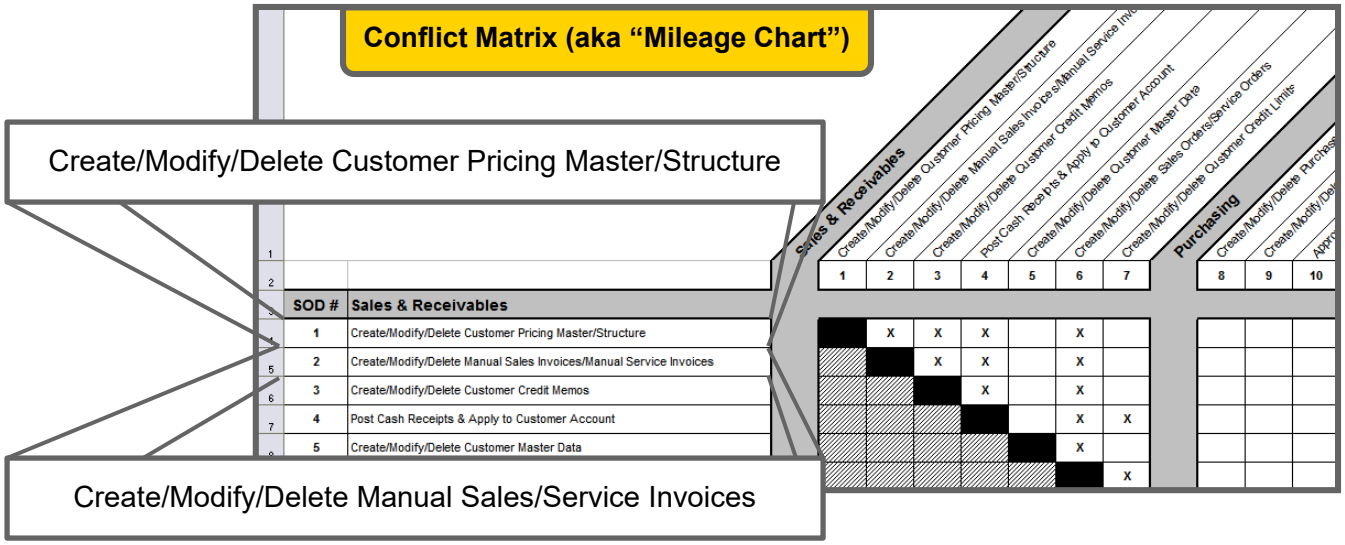
**Risk Statements**

**Business Definition** | Technical Definition | Testing | Mitigation | Remediation

# Create Conflict Matrix

- Determine SoD Program Objectives
- Define Sensitive Transactions
- Rank Sensitive Transactions According to Risk
- Determine Conflict Pairings and Establish Risk Ratings
- Create Risk (Impact) Statements
- **Create Conflict Matrix (aka "Mileage Chart")**

- The conflict matrix is a grid that displays the resulting conflicting sensitive transaction pairings on horizontal and vertical axes
- The matrix can be colored and organized according to the previously determined risk ratings




**Business Definition** | Technical Definition | Testing | Mitigation | Remediation

# Complete Application Applicability Chart

**Complete Application Applicability Chart**

Complete Application Testing Summary

Map Sensitive Transactions

Create Walkthrough of Application Security Model

Obtain System-Generated List of User Entitlements

- Determines where (which application) can execute each of the sensitive transactions
- Serves as input into the test plan
- Determines how testing is performed
- Illustrates the necessity for cross application conflict analysis
- does not complete the entire picture…

**Application-Applicability Chart**

| SOD Group | Sales & Receivables | Count of Mapped Access Rights | Application 1 | Application 2 | Application 3 | Application 4 |
|---|---|---|---|---|---|---|
| 1 | Create/Modify/Delete Customer Pricing Master/Structure | | 14 | 0 | 0 | 31 |
| 2 | Create/Modify/Delete Manual Sales Invoices/Manual Service Invoices | | 0 | 0 | 6 | 14 |
| 3 | Create/Modify/Delete Customer Credit Memos | | 0 | 0 | 5 | 19 |
| 4 | Post Cash Receipts & Apply to Customer Account | | 0 | 0 | 13 | 0 |
| 5 | Create/Modify/Delete Customer Master Data | | 2 | 0 | 9 | 7 |
| 6 | Create/Modify/Delete Sales Orders/Service Orders | | 4 | 0 | 5 | 24 |
| 7 | Create/Modify/Delete Customer Credit Limits | | 1 | 0 | 0 | 0 |
| | **Purchasing** | | | | | |
| 8 | Create/Modify/Delete Purchase Orders | | 0 | 0 | 6 | 0 |
| 9 | Create/Modify/Delete Vendor Master File Data | | 0 | 0 | 3 | 0 |
| 10 | Approve Purchase Orders | | 0 | 0 | 2 | 0 |
| | **Inventory Master Data** | | | | | |
| 11 | Create/Change Standard or Actual Costing | | 0 | 0 | 0 | 7 |
| 12 | Create/Change to Material Master Data | | 2 | 0 | 1 | 7 |
| | **Inventory Transactions** | | | | | |
| 13 | Record Inventory Movements or Production | | 0 | 0 | 0 | 32 |
| 14 | Record/Modify Shipment | | 1 | 0 | 0 | 0 |
| 15 | Receive/Post Physical Inventory or Cycle Counts | | 0 | 0 | 0 | 13 |
| | **Fixed Assets** | | | | | |
| 16 | Create/Modify/Delete Fixed Asset Records (Additions) | | 0 | 0 | 4 | 0 |
| 17 | Disposal/Retirement of Fixed Assets | | 0 | 0 | 2 | 0 |
| 18 | Depreciation of Fixed Assets | | 0 | 0 | 1 | 0 |

**Business Definition** | **Technical Definition** | **Testing** | **Mitigation** | **Remediation**

# Complete Application Testing Summary

- Complete Application Applicability Chart
- **Complete Application Testing Summary**
- Map Sensitive Transactions
- Create Walkthrough of Application Security Model
- Obtain System-Generated List of User Entitlements

- Illustrates the potential for cross application conflicts
- Determines where conflicts are not possible - due to system considerations - and therefore, should not be tested
- Verifies completeness of testing approach

**Application Testing Summary**

| Application | Application 1 | Application 2 | Application 3 | Application 4 |
|---|---|---|---|---|
| Application 1 | ✓ | ✓ | ✓ | ✓ |
| Application 2 | ■ | ✓ | ✓ | ✓ |
| Application 3 | ▨ | ■ | ✓ | ✓ |
| Application 4 | ▨ | ▨ | ■ | ✓ |

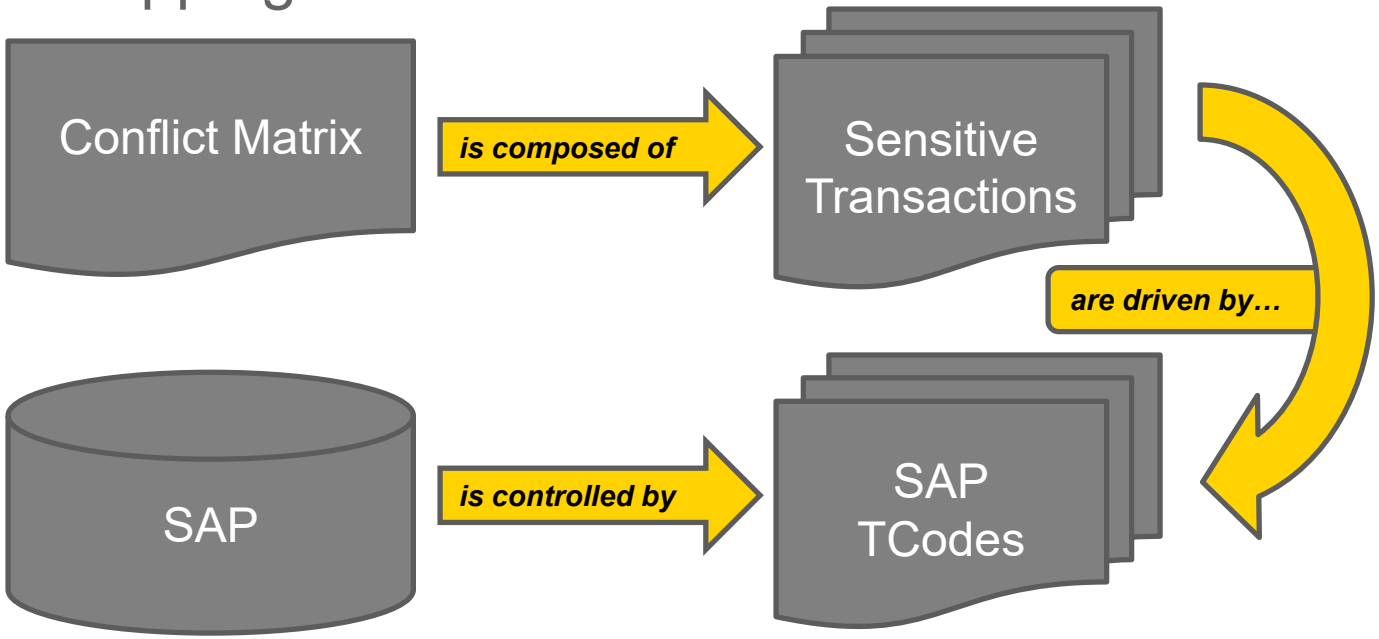
| Legend | |
|---|---|
| ✓ | SoD testing performed since potential conflicts identified. |
| × | SoD testing not performed since no potential for conflicts identified. |

**Business Definition** | **Technical Definition** | **Testing** | **Mitigation** | **Remediation**

# Map Sensitive Transactions to Lowest Level of Access

- Complete Application Applicability Chart
- Complete Application Testing Summary
- **Map Sensitive Transactions**
- Create Walkthrough of Application Security Model
- Obtain System-Generated List of User Entitlements

- Maps sensitive transactions to lowest level of security in each of the in-scope apps
- Potential for one-to-many relationship in mapping

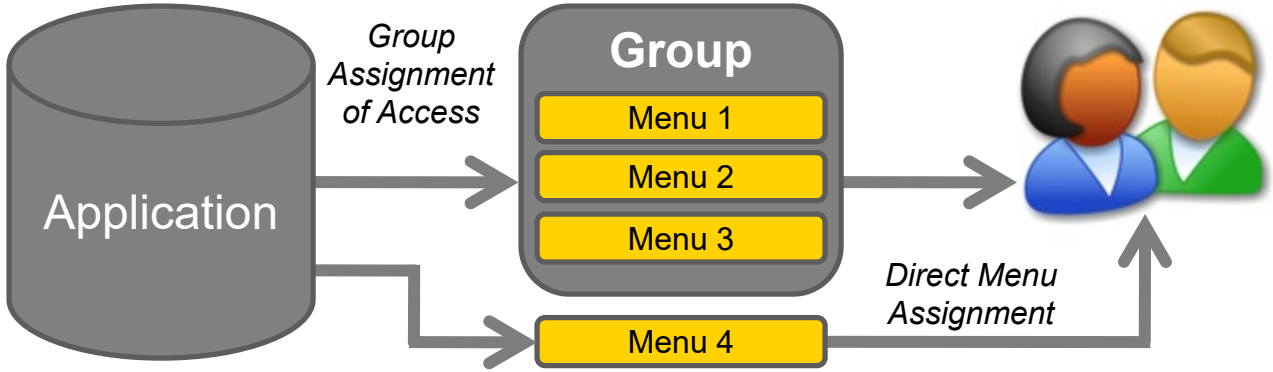



**Business Definition** | **Technical Definition** | **Testing** | **Mitigation** | **Remediation**

# Create Walkthrough of Application Security Model (Optional)

- Complete Application Applicability Chart
- Complete Application Testing Summary
- Map Sensitive Transactions
- **Create Walkthrough of Application Security Model**
- Obtain System-Generated List of User Entitlements

- Some applications may have obscure, non-standard, or hard-coded security models
- Legacy or home-grown applications may require a documented walkthrough to confirm understanding of the security model
- Existing documentations (SOX, financial audit, etc.) can be leveraged

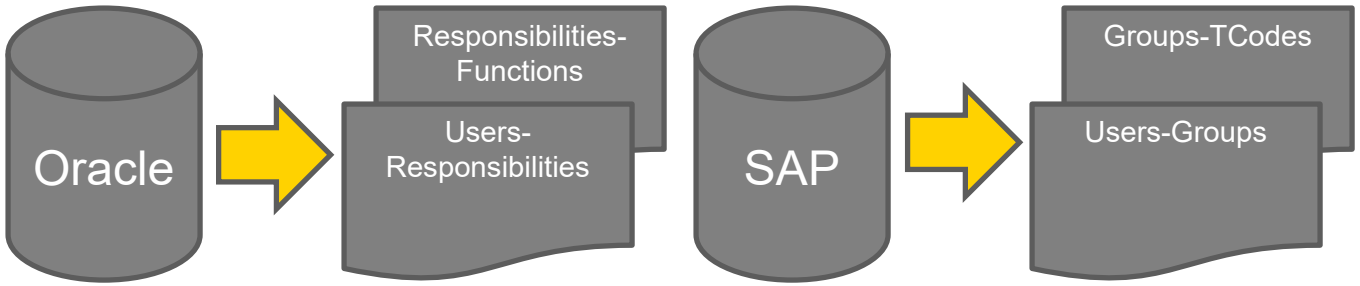



Business Definition | **Technical Definition** | Testing | Mitigation | Remediation

# Obtain System-Generated List of User Entitlements

- Complete Application Applicability Chart
- Complete Application Testing Summary
- Map Sensitive Transactions
- Create Walkthrough of Application Security Model
- **Obtain System-Generated List of User Entitlements**

- Export system generated list of:
  - *Users* mapped to their associated *application security group* (varies by application)
  - *Application security group* and its associated *access rights* that make up the group
- Important to analyze lowest level of security
- Watch out for direct user provisioning
- List should be obtained from *production*

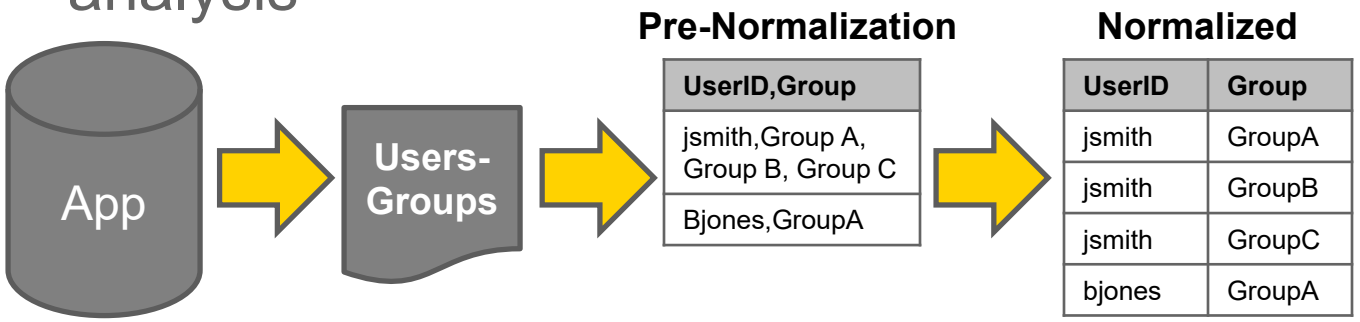



**Business Definition** | **Technical Definition** | **Testing** | **Mitigation** | **Remediation**

# Normalize System Generated Data

- **Normalize System Generated Data**
- Create SoD Test Plan
- Execute SoD Conflict Testing
- Perform Conflict Analysis
- Aggregate Conflict Counts
- Output Results to Conflict Matrix

- Normalization facilitates data analysis
- Application extracts are often formatted for display or report purposes
- If normalized extracts can not be natively obtained from the system, manual normalization is required
- Normalization is required for cross-application analysis




Business Definition | Technical Definition | **Testing** | Mitigation | Remediation

# Create SoD Test Plan

Normalize System Generated Data

**Create SoD Test Plan**

Execute SoD Conflict Testing

Perform Conflict Analysis

Aggregate Conflict Counts

Output Results to Conflict Matrix

- Test plan indicates the processes, sensitive transactions, and application where each test is to occur
- This should be done with a database, application or tool; very difficult to perform manually

**SoD Test Plan**

| ID | E | | | Application 1 | Business Process #2 | SOD #2 | Sensitive Transaction 2 | Application 2 |
|---|---|---|---|---|---|---|---|---|
| 1 | Sal | | icing | | | | | |
| 2 | Sales & Receivables | 1 | Master/Structure | | Sales & Receivables | 2 | Create/Modify/Delete Manual Sales Invoices/Manual Service Invoices | |
| 3 | Sales & Receivables | 1 | Create/Modify/Delete Customer Pricing Master/Structure | | Sales & Receivables | 2 | Create/Modify/Delete Manual Sales Invoices/Manual Service Invoices | |
| 4 | Sales & Receivables | 1 | Create/Modify/Delete Customer Pricing Master/Structure | | Sales & Receivables | 2 | Create/Modify/Delete Manual Sales Invoices/Manual Service Invoices | |
| 5 | Sales & Receivables | 1 | Create/Modify/Delete Customer Pricing Master/Structure | | Sales & Receivables | 2 | Create/Modify/Delete Manual Sales Invoices/Manual Service Invoices | |
| 6 | Sales & Receivables | 1 | Create/Modify/Delete Customer Pricing Master/Structure | | Sales & Receivables | 2 | Create/Modify/Delete Manual Sales Invoices/Manual Service Invoices | |
| 7 | Sales & Receivables | 1 | Create/Modify/Delete Customer Pricing Master/Structure | | Sales & Receivables | 3 | Create/Modify/Delete Customer Credit Memos | |
| 8 | Sales & Receivables | 1 | Create/Modify/Delete Customer Pricing Master/Structure | | Sales & Receivables | 3 | Create/Modify/Delete Customer Credit Memos | |
| 9 | Sales & Receivables | 1 | Create/Modify/Delete Customer Pricing Master/Structure | | Sales & Receivables | 3 | Create/Modify/Delete Customer Credit Memos | |
| 10 | Sales & Receivables | 1 | Create/Modify/Delete Customer Pricing Master/Structure | | Sales & Receivables | 3 | Create/Modify/Delete Customer Credit Memos | |
| 11 | Sales & Receivables | 1 | Create/Modify/Delete Customer Pricing Master/Structure | | Sales & Receivables | 3 | Create/Modify/Delete Customer Credit Memos | |
| 12 | Sales & Receivables | 1 | Create/Modify/Delete Customer Pricing Master/Structure | | Sales & Receivables | 3 | Create/Modify/Delete Customer Credit Memos | |
| 13 | Sales & Receivables | 1 | Create/Modify/Delete Customer Pricing Master/Structure | | Sales & Receivables | 4 | Post Cash Receipts & Apply to Customer Account | |
| 14 | Sales & Receivables | 1 | Create/Modify/Delete Customer Pricing Master/Structure | | Sales & Receivables | 4 | Post Cash Receipts & Apply to Customer Account | |
| 15 | Sales & Receivables | 1 | Create/Modify/Delete Customer Pricing Master/Structure | | Sales & Receivables | 4 | Post Cash Receipts & Apply to Customer Account | |
| 16 | Sales & Receivables | 1 | Create/Modify/Delete Customer Pricing Master/Structure | | Sales & Receivables | 6 | Create/Modify/Delete Sales Orders/Service Orders | |
| 17 | Sales & Receivables | 1 | Create/Modify/Delete Customer Pricing Master/Structure | | Sales & Receivables | 6 | Create/Modify/Delete Sales Orders/Service Orders | |
| 18 | Sales & Receivables | 1 | Create/Modify/Delete Customer Pricing Master/Structure | | Sales & Receivables | 6 | Create/Modify/Delete Sales Orders/Service Orders | |
| 19 | Sales & Receivables | 1 | Create/Modify/Delete Customer Pricing Master/Structure | | Sales & Receivables | 6 | Create/Modify/Delete Sales Orders/Service Orders | |
| 20 | Sales & Receivables | 1 | Create/Modify/Delete Customer Pricing Master/Structure | | Sales & Receivables | 6 | Create/Modify/Delete Sales Orders/Service Orders | |
| 21 | Sales & Receivables | 1 | Create/Modify/Delete Customer Pricing Master/Structure | | Sales & Receivables | 6 | Create/Modify/Delete Sales Orders/Service Orders | |

# Execute SoD Conflict Testing

Normalize System Generated Data

Create SoD Test Plan

**Execute SoD Conflict Testing**

Perform Conflict Analysis

Aggregate Conflict Counts

Output Results to Conflict Matrix

- Results of the testing are outputted to testing results spreadsheet
- Important to test each sensitive transaction and application combination

**SoD Test Plan**

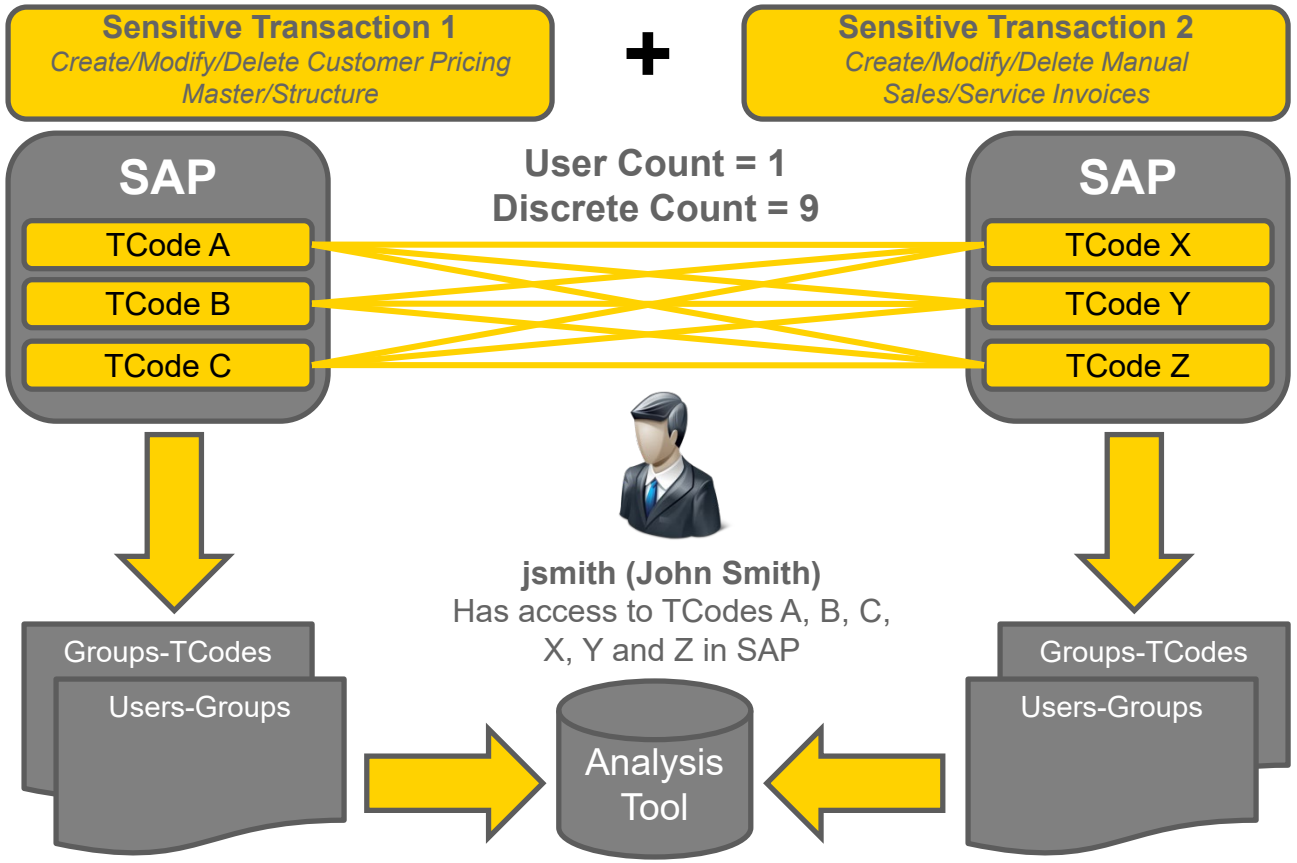
| Discrete Conflicts | User Conflicts | Role Conflicts |
|---|---|---|
| 27,840 | 4 | - |
| - | - | - |
| 1,214,886 | 87 | 24 |

**Business Definition** | **Technical Definition** | **Testing** | **Mitigation** | **Remediation**

# Perform Conflict Analysis

- Normalize System Generated Data
- Create SoD Test Plan
- Execute SoD Conflict Testing
- **Perform Conflict Analysis**
- Aggregate Conflict Counts
- Output Results to Conflict Matrix

## Example: Intra-Application Analysis

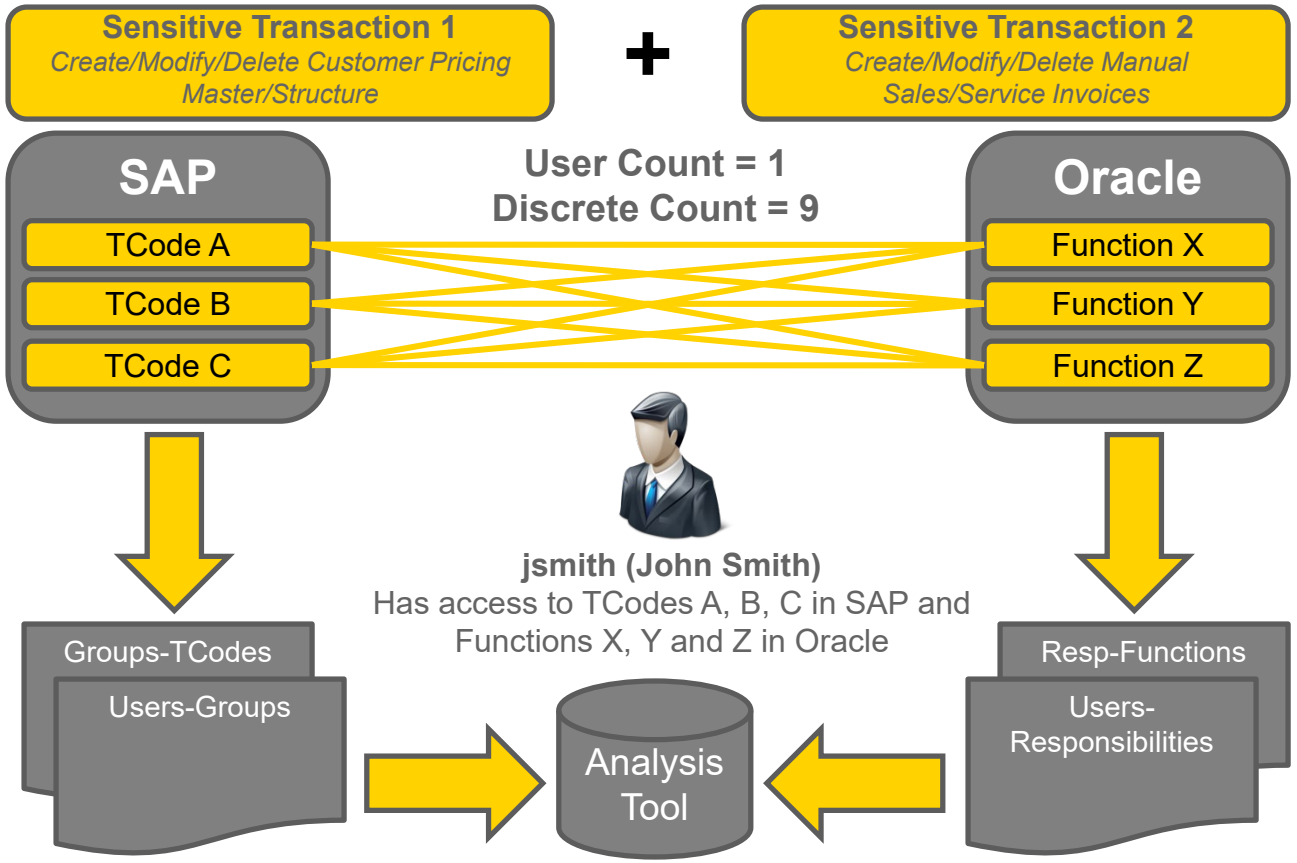



Business Definition | Technical Definition | **Testing** | Mitigation | Remediation

# Perform Conflict Analysis (Cont.)

- Normalize System Generated Data
- Create SoD Test Plan
- Execute SoD Conflict Testing
- **Perform Conflict Analysis**
- Aggregate Conflict Counts
- Output Results to Conflict Matrix

## Example: Cross Application Analysis




Business Definition | Technical Definition | **Testing** | Mitigation | Remediation

# Aggregate Conflict Counts

- Normalize System Generated Data
- Create SoD Test Plan
- Execute SoD Conflict Testing
- Perform Conflict Analysis
- **Aggregate Conflict Counts**
- Output Results to Conflict Matrix

| User | Discrete Count | Application 1 | SoD 1 | Application 2 | SoD 2 |
|---|---|---|---|---|---|
| jsmith | 9 | SAP | 1 | SAP | 2 |
| jsmith | 9 | SAP | 1 | Oracle Financials | 2 |
| jsmith | 9 | Oracle Financials | 1 | Oracle Financials | 2 |
| bjones | 16 | Oracle Financials | 1 | Oracle Financials | 2 |

- Conflict between SoD #1 (Create/Modify/Delete Customer Pricing Master/Structure) and SoD #2 (Create/Modify/Delete Manual Sales/Service Invoices):
  - **Discrete Conflicts:** 9 + 9 + 9 + 16 = 43 Discrete Conflicts
  - **User (Detailed) Conflicts:** jsmith + jsmith+ jsmith + bjones = 4 (Detailed) User Conflicts
  - **User (Collapsed) Conflicts:** jsmith + bjones = 2 (Collapsed) User Conflicts
- Collapsed user conflicts represents the most accurate report of *who* has access to *what* from an application-independent perspective
- Discrete and detailed counts are helpful when assessing magnitude and pervasiveness of the risk and are required for remediation activities

**Business Definition** | **Technical Definition** | **Testing** | **Mitigation** | **Remediation**

# Output Results to Conflict Matrix

- Normalize System Generated Data
- Create SoD Test Plan
- Execute SoD Conflict Testing
- Perform Conflict Analysis
- Aggregate Conflict Counts
- **Output Results to Conflict Matrix**

- Transfer testing results to conflict matrix
- Illustrates the number of users who have a conflict regardless of application

**SoD Test Plan**

| ID | | | | Application 1 | Business Process #2 | SOD #2 | Sensitive Transaction 2 | Application 2 | Discrete Conflictr | User Conflictr | Rule Conflictr |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Create/Modify/Delete Customer Pricing Master/Structure | | Sales & Receivables | 2 | Create/Modify/Delete Manual Sales Invoices/Manual Service Invoices | | 27,840 | 4 | - |
| 2 | Sales & Receivables | 1 | Create/Modify/Delete Customer Pricing Master/Structure | | Sales & Receivables | 2 | Create/Modify/Delete Manual Sales Invoices/Manual Service Invoices | | - | - | - |
| 3 | Sales & Receivables | 1 | Create/Modify/Delete Customer Pricing Master/Structure | | | | Create/Modify/Delete Manual Sales | | | | 24 |
| 4 | Sales & Receivables | 1 | Create/Modif Master/Struc | | | | | | | | - |
| 5 | Sales & Receivables | 1 | Create/Modif Master/Struc | | | | | | | | - |
| 6 | Sales & Receivables | 1 | Create/Modif Master/Struc | | | | | | | | 1 |
| 7 | Sales & Receivables | 1 | Create/Modif Master/Struc | | | | | | | | - |
| 8 | Sales & Receivables | 1 | Create/Modif Master/Struc | | | | | | | | - |
| 9 | Sales & Receivables | 1 | Create/Modif Master/Struc | | | | | | | | 24 |
| 10 | Sales & Receivables | 1 | Create/Modif Master/Struc | | | | | | | | - |
| 11 | Sales & Receivables | 1 | Create/Modif Master/Struc | | | | | | | | - |
| 12 | Sales & Receivables | 1 | Create/Modif Master/Struc | | | | | | | | 1 |

**Conflict Matrix (Populated)**

Total User Conflict Count = 7,063

| SOD # | Sales & Receivables | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| 1 | Create/Modify/Delete Customer Pricing Master/Structure | | 122 | 122 | 83 | | 74 | |
| 2 | Create/Modify/Delete Manual Sales Invoices/Manual Service Invoices | | | 627 | 87 | | 487 | |
| 3 | Create/Modify/Delete Customer Credit Memos | | | | 82 | | 486 | |
| 4 | Post Cash Receipts & Apply to Customer Account | | | | | | 33 | 4 |
| 5 | Create/Modify/Delete Customer Master Data | | | | | | 656 | |
| 6 | Create/Modify/Delete Sales Orders/Service Orders | | | | | | | 43 |
| 7 | Create/Modify/Delete Customer Credit Limits | | | | | | | |
| | **Purchasing** | | | | | | | |
| 8 | Create/Modify/Delete Purchase Orders | | | | | | | |
| 9 | Create/Modify/Delete Vendor Master File Data | | | | | | | |
| 10 | Approve Purchase Orders | | | | | | | |

| | | | | |
|---|---|---|---|---|
| Business Definition | Technical Definition | **Testing** | Mitigation | Remediation |

# Mitigation Objective

- After conflicts have been tested and analyzed, a common question arises:

**What do we do now?**

- The purpose of mitigating controls phase is to expose the remaining, residual risk of the noted conflicts
- Residual risk can be minimized through remediation techniques and implementation of additional financial controls

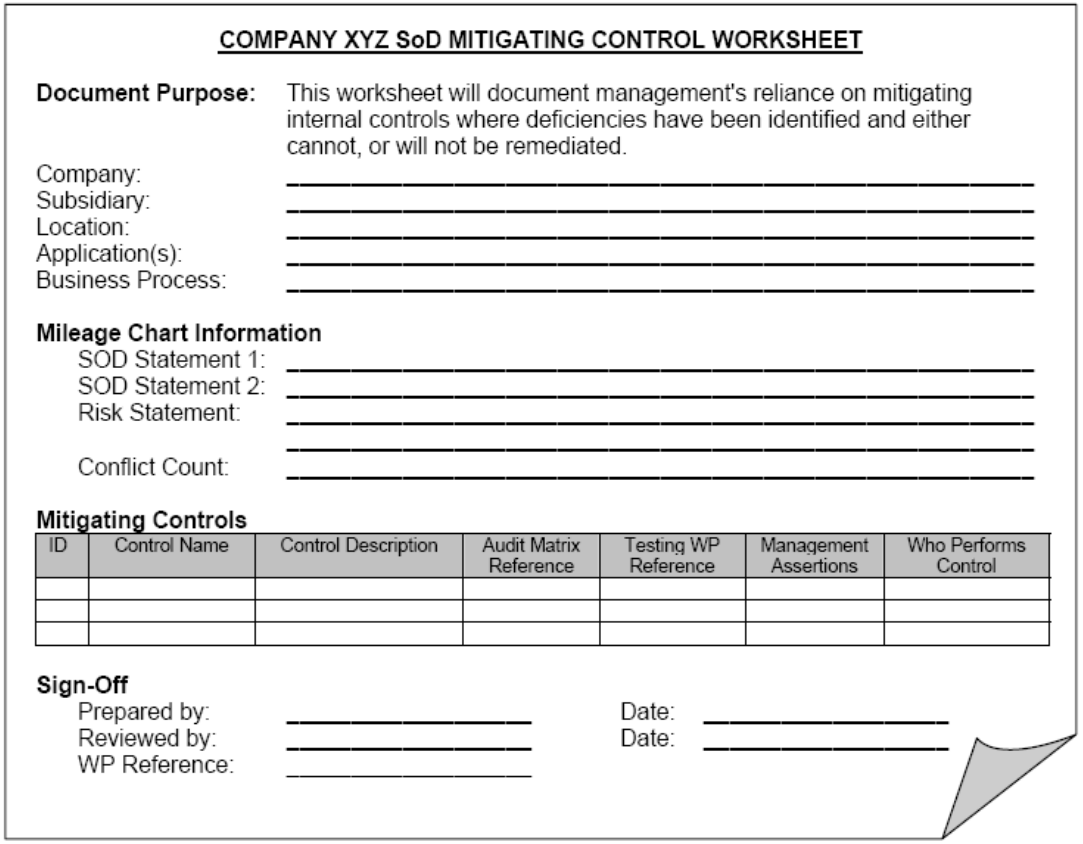
**Assessed SoD Risk**
**(Financial Controls)**
**Residual Risk**

- The business can often cite existing financial controls and focus its time and attention on remediating the highest risk conflicts

Business Definition | Technical Definition | Testing | **Mitigation** | Remediation

# Mitigating Controls Documentation

- Mitigation performed at the business process/sensitive transaction level
- Every intersection should have adequate mitigating controls, but only the intersections with conflicts are required
- Mitigating controls are cited from the key financial controls
- Control should have passed internal audit testing
- "Auditor Judgment" is general standard for adequacy of mitigation of the risk
- Thumb rule: 2+ controls are better than 1



**COMPANY XYZ SoD MITIGATING CONTROL WORKSHEET**

**Document Purpose:** This worksheet will document management's reliance on mitigating internal controls where deficiencies have been identified and either cannot, or will not be remediated.

Company: _____
Subsidiary: _____
Location: _____
Application(s): _____
Business Process: _____

**Mileage Chart Information**

SOD Statement 1: _____
SOD Statement 2: _____
Risk Statement: _____
_____
Conflict Count: _____

**Mitigating Controls**

| ID | Control Name | Control Description | Audit Matrix Reference | Testing WP Reference | Management Assertions | Who Performs Control |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |

**Sign-Off**

Prepared by: _____ Date: _____
Reviewed by: _____ Date: _____
WP Reference: _____

Business Definition | Technical Definition | Testing | **Mitigation** | Remediation

# Mitigating Controls Tips

- Mitigating controls must have passed internal audit testing
- Watch for *fox-and-henhouse* conflicts
  - The reviewer and/or approver of the mitigating control cannot be in the conflicted population
  - If this condition exists, the control must either be assigned to someone else to perform or the conflict must be corrected
- Detective controls are good, but preventive controls are better; should strive for a good mix
- Management assertions (CAVR*) of the control should be complementary to the management assertion of the conflict
- Entity-level and budget-to-actual reconciliation controls should not be overused
- It is important to document the rationale for selection of the mitigating control since auditor judgment dictates whether the controls mitigate the risk of the conflict

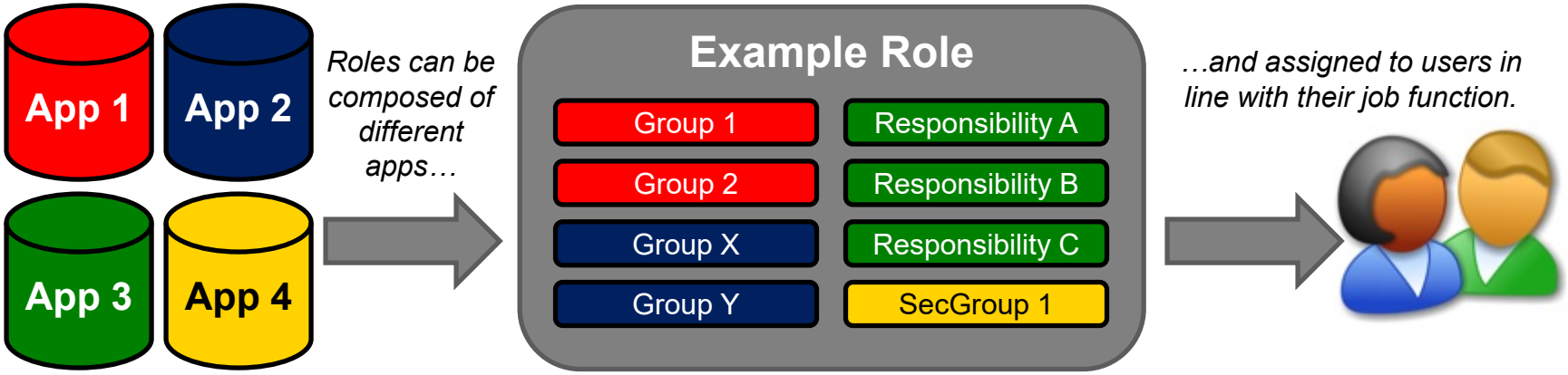
* CAVR: Completeness, Accuracy, Validity, and Restricted Access

# Remediation Overview

- Remediation seeks to permanently correct the issues noted in testing
- Initiatives can be prioritized to tactically address the high-risk and/or unmitigated conflicts
- Long-term solutions should consider
  - **People** – Cultural changes, training, education and awareness is required; sometimes being *helpful* introduces conflicts
  - **Process** – Processes (provisioning, de-provisioning, access changes, etc.) often need to be changed to ensure conflicts are not reintroduced after cleanup
  - **Technology** – Third-party tools and applications make compliance sustainability easier

# Common Remediation Techniques

- Role-based access control (intelligence in the role)
- Approval-based access control (intelligence in the tool)
- User appropriateness review and verification
- Third-party tool implementation and integration
- Business process redesign and workflow
- Meta-directory implementation



# SoD Tools and Applications

- Third-party tools are helpful, but not all tools are created equally
- Gartner MarketScope for Segregation of Duty Controls Within ERP and Financial Applications (September 2008)*

| | RATING | | | | |
|---|---|---|---|---|---|
| | Strong Negative | Caution | Promising | Positive | Strong Positive |
| Approva | | | | | x |
| Control Software International | | | x | | |
| Fox Technologies | | x | | | |
| Oracle | | | | x | |
| SAP | | | | x | |
| Security Weaver | | | | x | |
| Sun Microsystems | | | x | | |

As of 25 September 2008

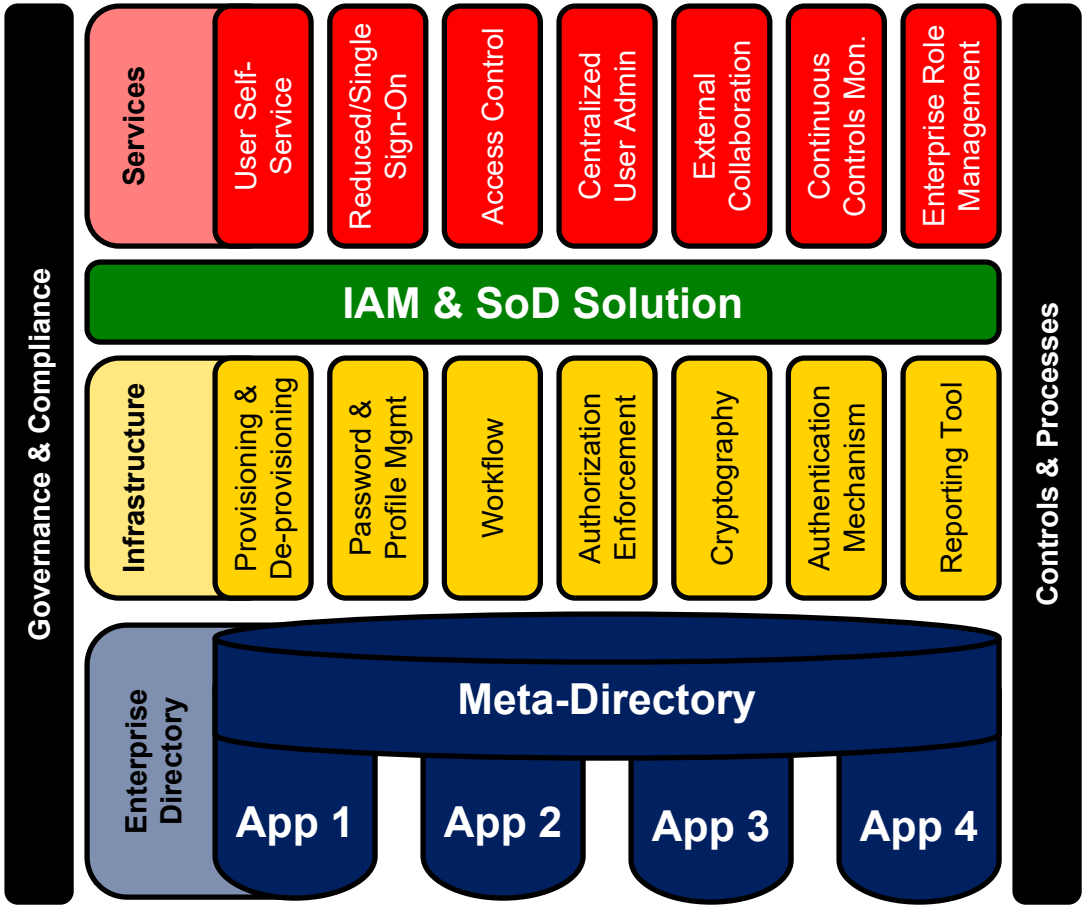
- A tool is not a replacement for a coherent SoD approach
- Many tools have pre-defined conflicts, but still need to be adapted to the business model and processes to prevent false positives
- Cross-application analysis is still a challenge for many tools

* Source: http://response.approva.net/content/GartnerMarketScopeAE

Business Definition | Technical Definition | Testing | Mitigation | **Remediation**

# Identity & Access Management

- SoD is difficult without a master record source and single view of the user (Meta-Directory)
- SoD can be built into an IAM solution that sits on top of the infrastructure
- Leading IAM practices that enable SoD:
  - User ID consistency
  - Workflow for access approval
  - Mitigating controls integration into approval process
  - Logging and monitoring of powerful accounts
  - Prevent and detect controls
  - Collusion detection




Business Definition | Technical Definition | Testing | Mitigation | Remediation

A Risk-Based Approach to Segregation of Duties

# LESSONS LEARNED

# Managing the Stakeholders

## Working with IT

- Accountability is essential: executive sponsorship is required
- Engage IT early & often – compliance is difficult when IT is brought in late in the process
- Some IT stakeholders have very detailed knowledge of the business process flows in the system
- Do not assume a system has all functionality to remediate; always confirm
- IT SoD (super users, powerful users, developer access to production, etc.) is a separate issue and can be tested in IT general controls (ITGCs)

## Working with the Business

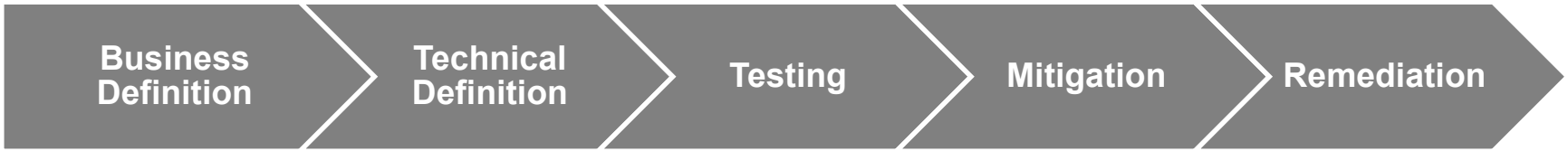
- Accountability is essential: executive sponsorship is required
- The business (finance, accounting, operations, etc.) typically knows the processes the best, but may not understand all the avenues for a potential transaction
- Business is responsible for the business requirements definition; IT enforces the access in the application

# Managing the Stakeholders (Cont.)

## Working with External Audit

- **Communicate**
  - Establish periodic check-points and meetings to review progress and milestones
- **Plan**
  - Co-develop testing schedules and time lines
- **Manage expectations**
  - Discuss issues and their potential consequences (deficiency, significant deficiency, etc.), but compile a management position or opinion on the assessment of the issues
- **Periodic testing**
  - SoD is not a point-in-time compliance check, it should be tested periodically
- **Leverage internal audit & management testing**
  - If approach is sound, external audit may simply choose to re-perform testing
- **Verify buy-in on approach and assumptions**
  - Each case is unique; buy-in on the approach is critical to avoiding surprises

# Conclusion

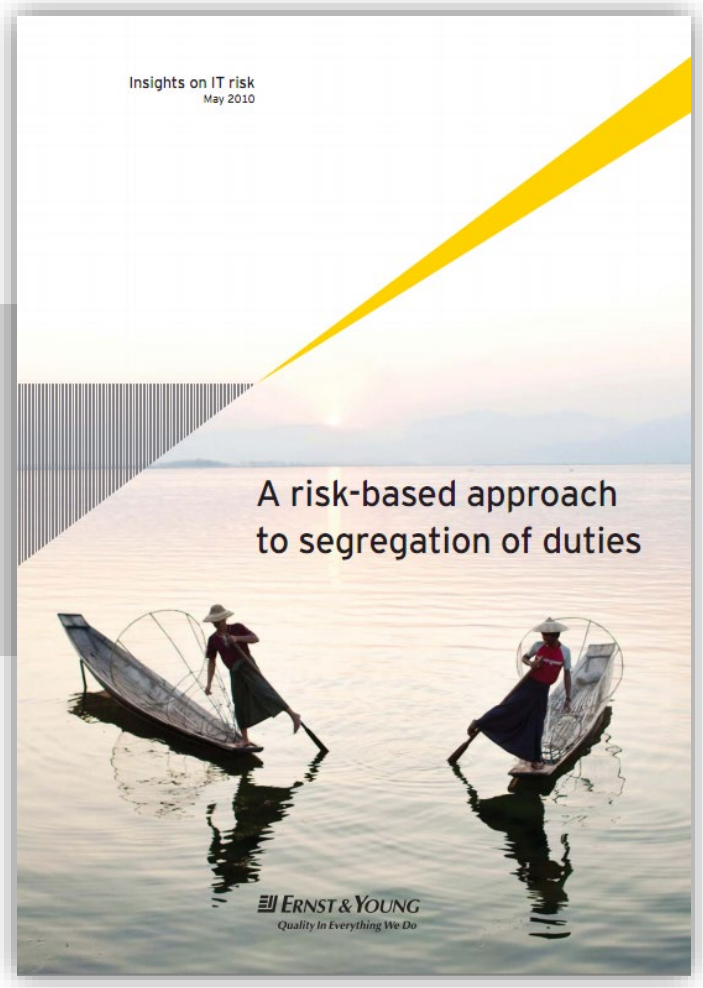



- Proper ownership and governance is essential
- A risk-based approach can accommodate most any sized organization
- Mitigation is an effective risk-management technique
- Remediation can be flexible and suited to the organization's needs and priorities
- Compliance is possible with planning, communication and a sound approach

Experience can make the difference between a minor issue and a material weakness. Don't go at it alone; help is available.

# More information available on ey.com

http://www.ey.com/Publication/vwLUAssets/Insights_on_IT_risk_-_05_2010_-_Risk-based_approach_to_segregation_of_duties/$FILE/EY_Insights_on_IT_risk_05_2010_-_Segregation_of_duties.pdf



# Contact Information

**Justin Greis**
Senior Manager
Chicago, Illinois

Phone: +1 (312) 342-4202
E-Mail: justin.greis@ey.com

**Chris Hansen**
Manager
New York, New York

Phone: +1 (212) 773-0444
E-Mail: chris.hansen@ey.com

# Thank You

ISACA Charlotte SoD Discussion

28 October 2011

Ernst & Young

Quality In Everything We Do

A Risk-Based Approach to Segregation of Duties

# APPENDIX: SOD PROJECT PHASES

# Strategy & Vision

**Typical Duration**
3 - 4 Weeks

**Input**

- Application portfolio & architecture map
- Business process documentation
- Key control framework/matrices
- Stakeholder listing

**Process**

- Stakeholder interviews and facilitated sessions
- Project planning and scheduling
- Application scoping and technical review
- Business process, business unit and geographic scoping
- Key financial control review
- Internal [and external audit] meeting scheduling

**Output**

- Segregation of Duties (SoD) strategy & vision document
- Segregation of Duties (SoD) roadmap and high-level project plan
- Segregation of Duties (SoD) project charter
- Segregation of Duties (SoD) program management office (PMO)
- Segregation of Duties (SoD) draft templates package

## Key Benefits

- Executive and internal stakeholder buy-in
- Preliminary scope and project planning
- SoD PMO established to coordinate activities
- Draft templates to provide documentation standard throughout project

## Key Dependencies

- Executive sign-off of scope and approach
- Internal and external audit scope agreement

**Strategy & Vision** | Business Definition | Technical Definition | Testing | Mitigation | Remediation

# Business Definition

**Typical Duration**
2 - 4 Weeks

**Input**

- Segregation of Duties (SoD) strategy & vision document
- Segregation of Duties (SoD) roadmap and high-level project plan
- Segregation of Duties (SoD) project charter
- Segregation of Duties (SoD) program management office (PMO)
- Segregation of Duties (SoD) draft templates package
- Standard/industry conflict matrices/pairings

**Process**

- Materiality and conflict financial threshold calculations
- Business process walkthroughs and documentation review
- Business process owner facilitated sessions to discuss potential for fraudulent activities within the customized processes
- Conflicting transaction risk analysis and ranking

**Output**

- Sensitive business transactions and SoD conflict matrix/pairings (aka "Mileage Chart")
- Conflict pairing risk analysis and materiality threshold calculation
- Risk-ranked SoD conflicts (e.g. high, medium, low, etc.)
- Risk statements for each SoD conflicts

## Key Benefits

- Understanding of the business SoD conflicts
- Organization's tolerance for risk associated with each conflict
- Clear level of materiality associated with each SoD conflict
- SoD matrix that will drive the subsequent project phases

## Key Dependencies

- Clear understanding of the business transactions and any unique or uncommon business processes
- Agreement with audit parties on appropriate materiality
- Documentation of existing processes

Strategy & Vision | **Business Definition** | Technical Definition | Testing | Mitigation | Remediation

# Technical Definition

**Typical Duration**
4 - 6 Weeks

**Input**

- SoD conflict matrix
- SoD risk statement listing
- Preliminary application scope (i.e. key financial systems)
- Standard/Industry access security mappings

**Process**

- Business process application and screen walkthrough
- IT and administrator walkthroughs of alternate security/functionality enabling sensitive transactions
- Custom functionality walkthrough meetings

**Output**

- Application-applicability chart and application testing summary
- Application access rights mapped to sensitive transactions defined in the SoD conflict matrix
- Application security model walkthrough (as needed) for legacy or custom applications
- User entitlement listings from the in-scope production applications

## Key Benefits

- Clear understanding of what application access rights correspond to the associated business process
- Clear application scope for future testing phases
- Plan for where cross-application conflicts may exist

## Key Dependencies

- Limitation of scope for low-risk or smaller dollar-value applications
- Legacy applications or custom security models can be mapped (i.e. security is not hard-coded into the functionality)
- Lowest level of security should be mapped to sensitive transactions; not roles/groups

Strategy & Vision | Business Definition | **Technical Definition** | Testing | Mitigation | Remediation

# Testing

**Typical Duration**
2 - 4 Weeks

**Input**

- Application access rights mapped to sensitive transactions defined in the SoD conflict matrix
- User entitlement listings from the in-scope production applications

**Process**

- Creation of SoD test plan
- Intra- and cross-application SoD testing for defined set of conflicts
- Normalization of system-generated production data
- Configuration of SoD conflict rules within testing tool
- Analysis and aggregation of various user conflict reports

**Output**

- User conflict reports (e.g. by application, role, process, user, etc.)
- Populated SoD conflict matrix with consolidated user conflict counts
- Consolidated management testing package

## Key Benefits

- Reveals users with defined SoD conflicts
- Quantifies risk of SoD among the user population
- Creates metrics and allows for monitoring and trending of user conflicts over time
- Demonstrates level of control over issue by revealing users with conflicts

## Key Dependencies

- Ability to produce and analyze massive amounts of data
- Testing tool is key to sustaining compliance after initial testing phase
- If applicable, implementation of SoD tool should begin in previous phase
- Clear definition of SoD conflicts

Strategy & Vision | Business Definition | Technical Definition | **Testing** | Mitigation | Remediation

# Mitigation

**Typical Duration**
3 - 4 Weeks

**Input**

- Preliminary SoD conflict matrix
- Populated SoD conflict matrix with consolidated user conflict counts (*optional*)
- Consolidated management testing package (*optional*)

**Process**

- Review of key financial controls and citation of mitigating controls that compensate for the risk of the potential SoD conflicts
- Justification for the selection of each control and combination of controls as to why the do/do not mitigate the SoD conflict
- Matching of management assertion (CAVR) of the control to the SoD conflict

**Output**

- Mitigating control worksheets for each identified SoD conflict
- Mitigating control package and audit documentation
- Listing of fox & henhouse scenarios for priority remediation
- If applicable, recommendations for new/additional controls to be added to the control framework

## Key Benefits

- Provides a “safety net” of controls in place in the event of an unfixable SoD conflict
- Provides an ongoing framework for prioritizing levels of controls for testing
- Reveals areas of opportunity to strengthen internal controls
- Demonstrates a level of comfort that identified conflicts do not pose a business risk

## Key Dependencies

- Completeness of internal financial controls and framework
- Relied upon controls should be tested and passed testing
- “Fox & henhouse” scneario
- Combination of detective & preventive controls

Strategy & Vision | Business Definition | Technical Definition | Testing | **Mitigation** | Remediation

# Remediation

**Typical Duration**
4 - 6+ Weeks

**Input**

- User conflict reports (e.g. by application, role, process, user, etc.)
- Populated SoD conflict matrix with consolidated user conflict counts
- Mitigating control worksheets for each identified SoD conflict
- Mitigating control package and audit documentation
- Conflict risk rating for each SoD conflict

**Process**

- Appropriate access reviews
- Role redesign and/or cleanup
- Implementation of SoD and/or Identity & Access Management tool
- Provisioning/De-provisioning process redesign

**Output**

- Sustainable process for maintaining environment where SoD conflicts have been minimized (to the greatest extent possible)
- Clean (i.e. conflict-free) roles and user population
- Revised access request processes with built-in conflict checks and mitigation processes based on tested/passed internal controls

## Key Benefits

- Minimizes conflicts
- Attempts to eliminate conflicts that cannot be mitigated
- Aligns systems roles or access to organizational functions

## Key Dependencies

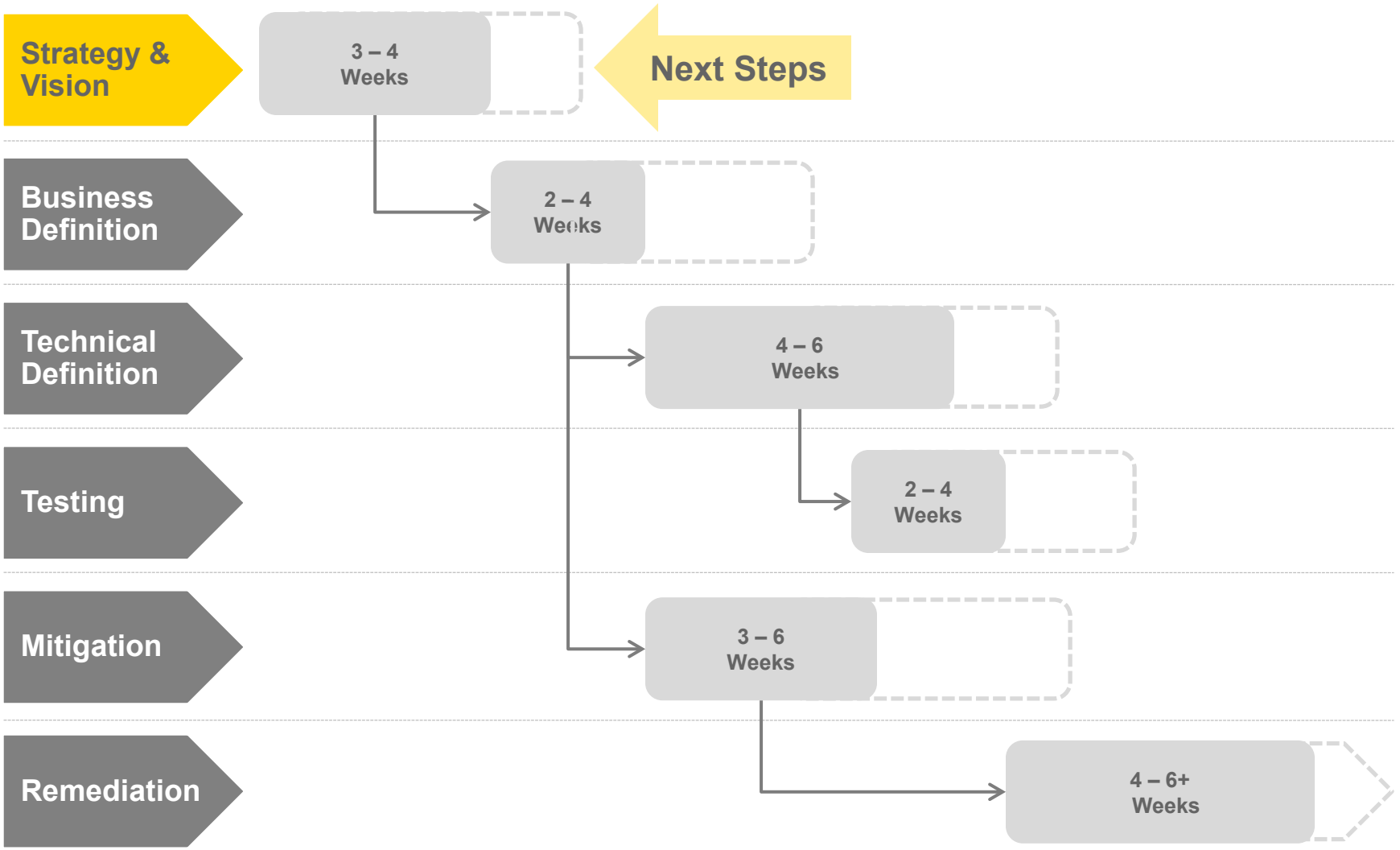
- Identification of detailed discrete conflicts by application, module, role, user, etc.
- SoD tool can assist in remediation/cleanup activities
- Management desire to pursue cleanup or mitigation strategy

## Important Note

Remediation initiatives vary from client-to-client and scenario-to-scenario. Conflict levels will determine the scope and extent of remediation initiatives required.

Strategy & Vision → Business Definition → Technical Definition → Testing → Mitigation → **Remediation**

# Typical SoD Project Time Line



# Scoping Information Required

| Information Required | Response |
|---|---|
| Number of business units in scope | |
| Preliminary number of key applications and modules in-scope | |
| Name and version of in-scope applications | |
| Any IAM/SoD tools currently in-use at your company | |
| In-scope geographies or regions | |
| Financial year-end and key internal/external audit meeting dates | |
| Control testing time lines | |
| Key contacts and stakeholders | |