A Risk-Based Approach to Segregation of Duties

ISACA®

2010 North America CACS Conference Session

19 April 2010

Trust in, and value from, information systems

Introductions

Michael Adolphson

Senior Manager
Advisory Services
St. Louis, Missouri

- BS ‘96 (Accounting)
- CISA, CISM, CPA, CISSP
- Frequent guest lecturer at Northern Illinois University and Indiana University, Bloomington
- Specializations
  - IT and Business Process Improvement
  - Segregation of Duties
  - Identity & Access Management
  - Information Security
  - IT Audit (Internal & External)

Justin Greis

Manager
Advisory Services
Chicago, Illinois

- BS ‘03, MBA ‘04 (Accounting/IS)
- CISA, CISM, CGEIT, CISSP, CIPP, GIAC/GSEC, PMP, ITIL
- Adjunct 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

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?

ISACA® Trust in, and value from, information systems

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
6. Perform an exercise to apply lessons learned

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

Trust in, and value from, information systems

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
  - 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.

Stakeholders

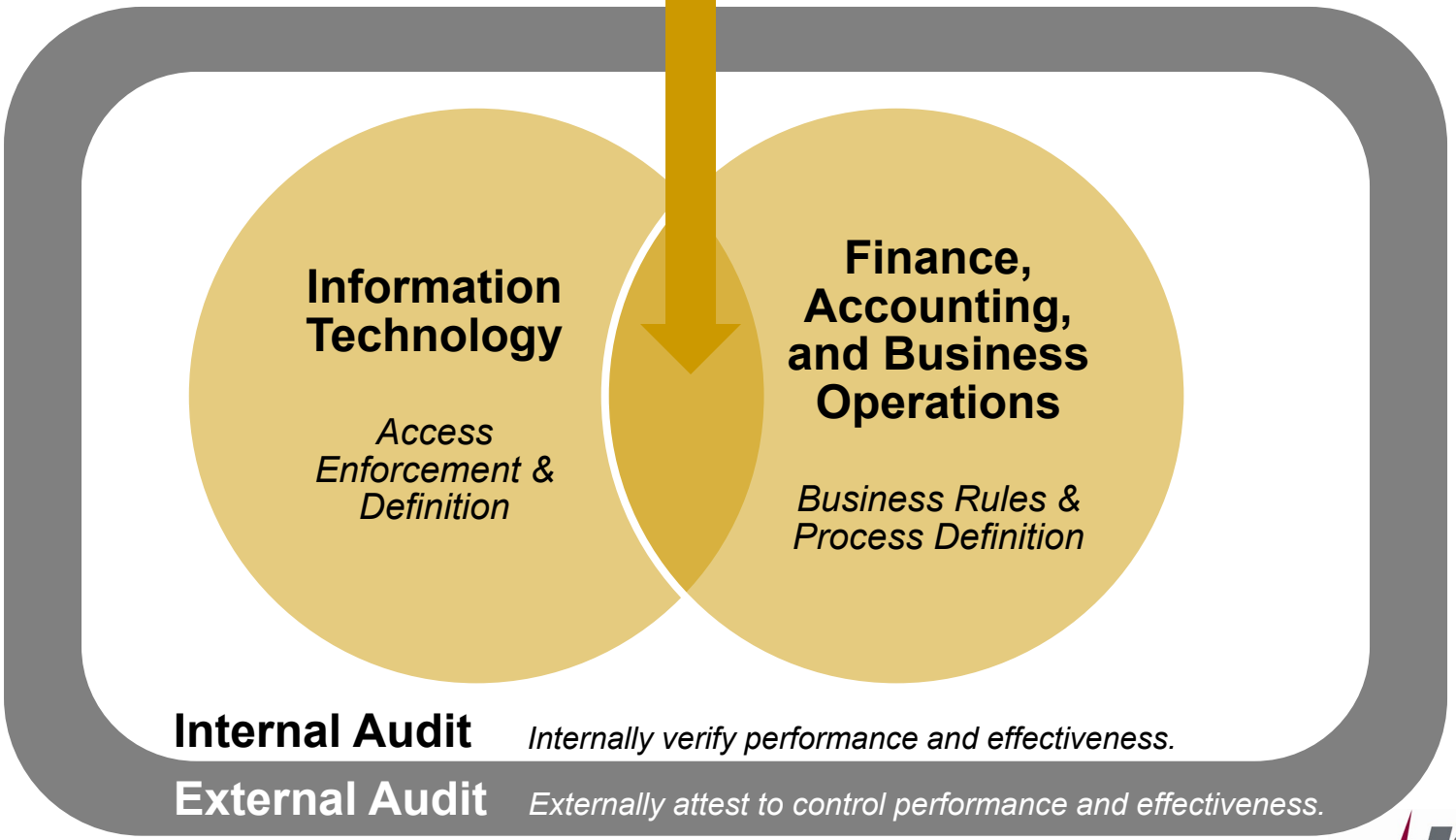
- **CFO & CIO** – Leadership must support business process reengineering and/or changes to control structure in order to remediate/mitigate SoD control failures
- **Internal Audit/Compliance** – Internal audit/compliance can assist with testing and mitigating control documentation
- **Business Finance 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

Important Successful SoD governance exists as a partnership between IT and the business



Trust in, and value from, information systems

A Risk-Based Approach to Segregation of Duties

SOD METHODOLOGY & APPROACH

Trust in, and value from, information systems

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 | Inspections

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

Washington, DC, December 5, 2006 – The Public Company Accounting Oversight Board has announced an open meeting for 9:30 a.m. Tuesday, December 19, to consider proposing for public comment a new auditing standard to supersede the Board's existing auditing standard on internal control over financial reporting, and other related proposals.

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

"The Sarbanes-Oxley Act's internal control requirements have been described as the most significant change in public company auditing since the advent of the federal securities laws," said Chairman Mark Olson. "While the requirements provide great benefits to companies and their investors, we are concerned that the costs are not adequately aligned with the benefits. For its part, the PCAOB will consider changes to the auditing standard on internal control over financial reporting that provide for a much more efficient, risk-based, scalable implementation. It is important that investors, companies, and auditors carefully consider and provide comments on the new proposal so that we reach the right result."

"The PCAOB is applying what it has learned in two years of monitoring the implementation of Auditing Standard No. 2, to help auditors make their internal control audits as efficient as possible while maintaining the benefits to investors," said Tom 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

Trust in, and value from, information systems

Determine Program Objectives

- **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")

- 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

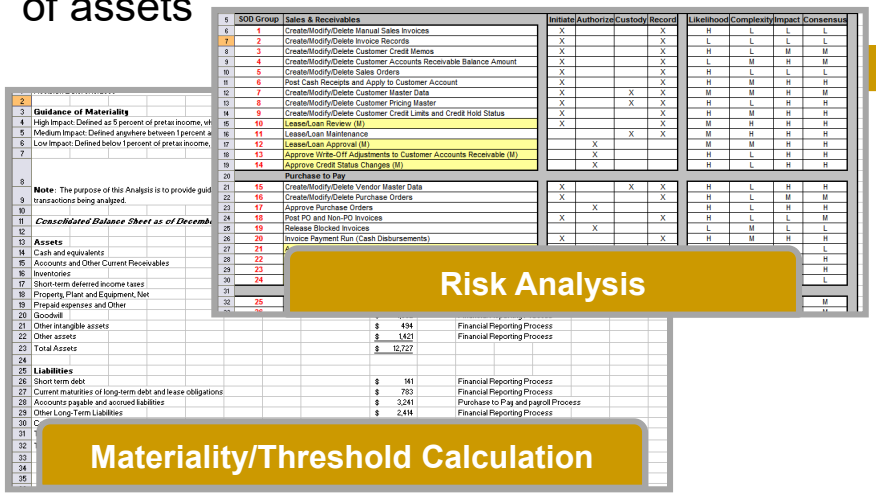
Business Definition | Technical Definition | Testing | Mitigation | Remediation

ISACA® Trust in, and value from, information systems

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

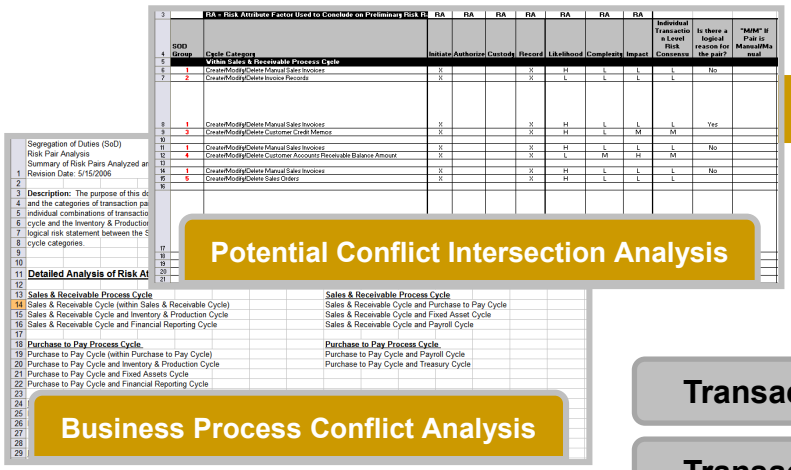
Business Definition → Technical Definition → Testing → Mitigation → Remediation

ISACA® Trust in, and value from, information systems

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

ISACA® Trust in, and value from, information systems

Determine Conflict Pairings and Establish Risk Ratings (Cont.)

- 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")

- 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

- 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**

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")

	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 & Receivab						A user could modify pricing terms and manipulate sales/service orders to offer favorable pricing for the customer.
5	Sales & Receivab						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 & Receivab		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

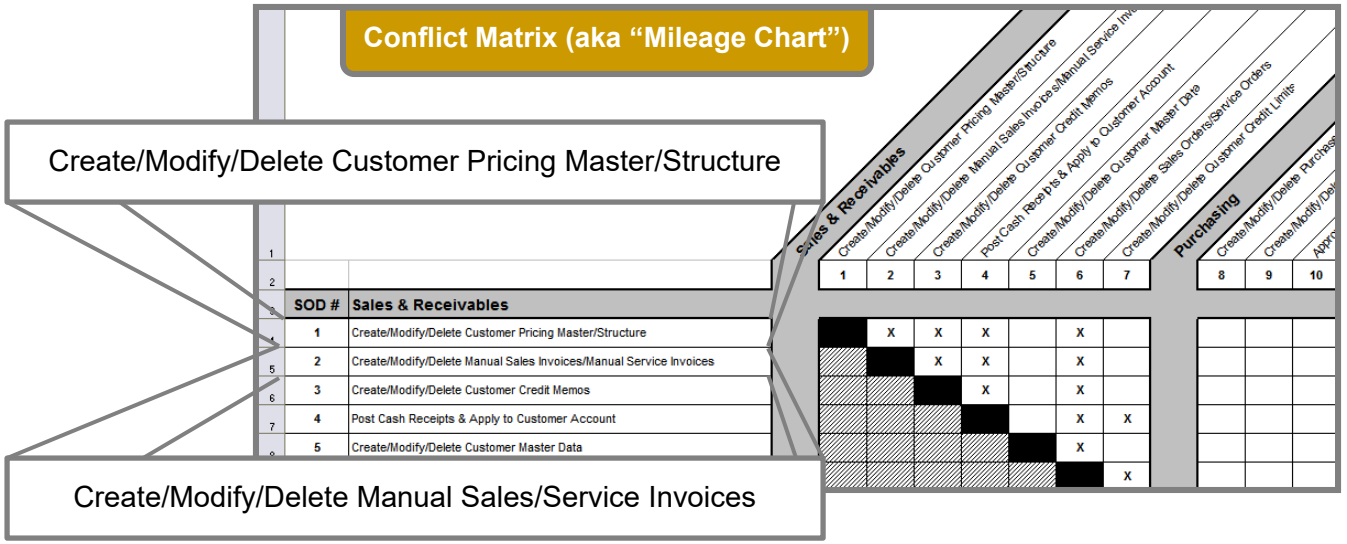
Business Definition | Technical Definition | Testing | Mitigation | Remediation

ISACA® Trust in, and value from, information systems

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

ISACA® Trust in, and value from, information systems

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

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	▨	▨	■	✓

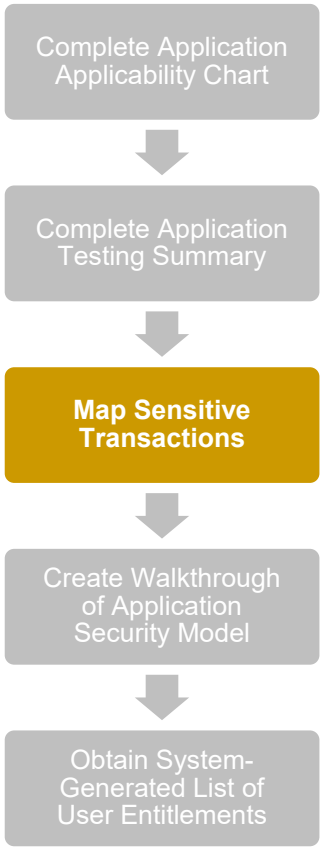
Legend	
✓	SoD testing performed since potential conflicts identified.
×	SoD testing not performed since no potential for conflicts identified.

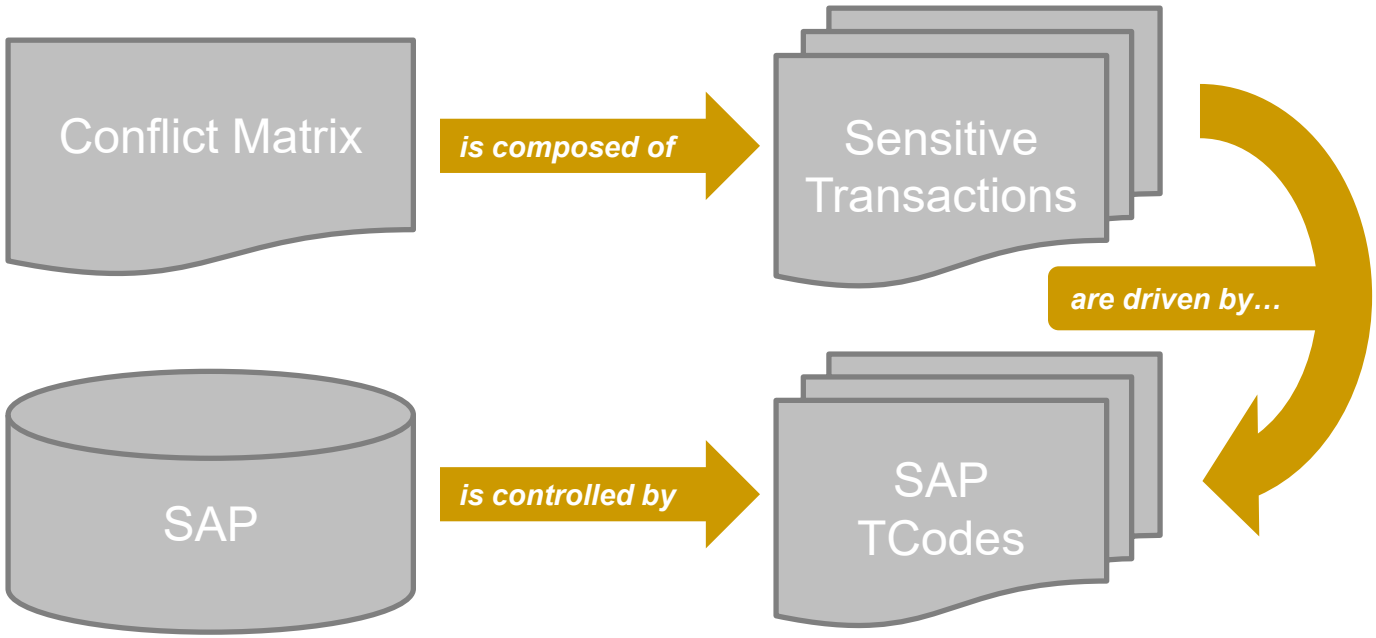
Business Definition | **Technical Definition** | Testing | Mitigation | Remediation

Trust in, and value from, information systems

Map Sensitive Transactions to Lowest Level of Access

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



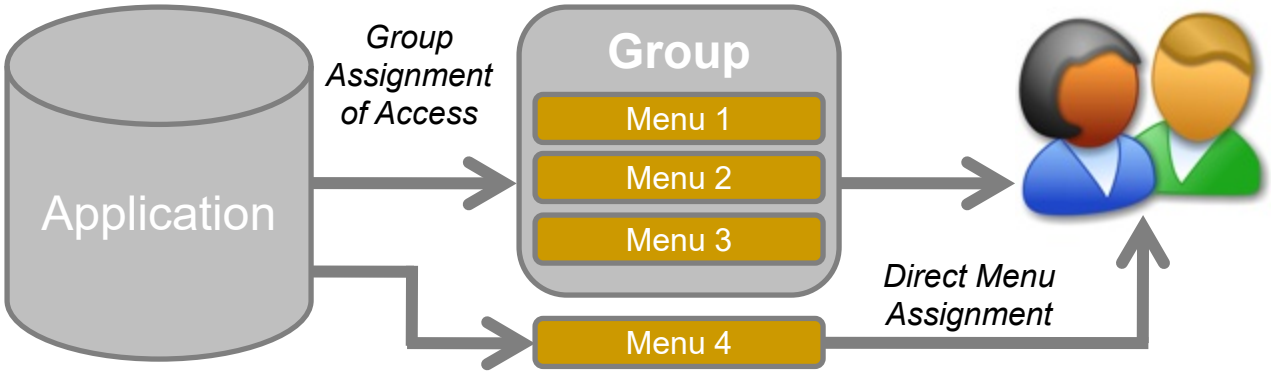


Trust in, and value from, information systems

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



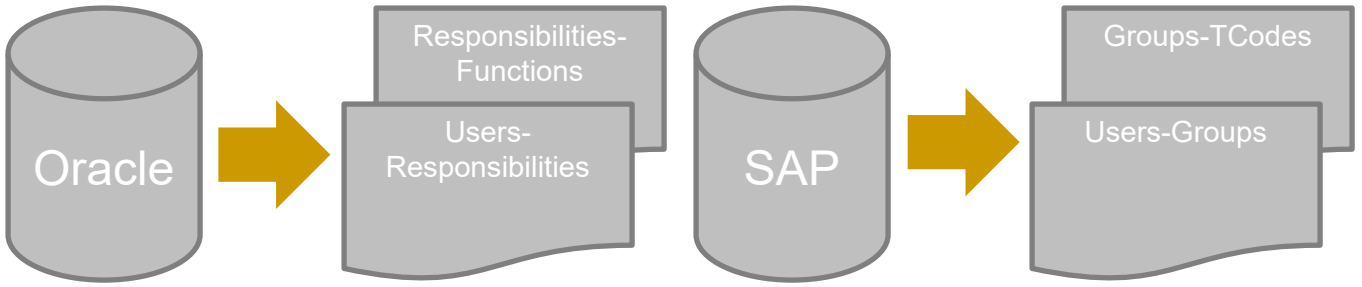
Business Definition | **Technical Definition** | Testing | Mitigation | Remediation

ISACA® Trust in, and value from, information systems

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*

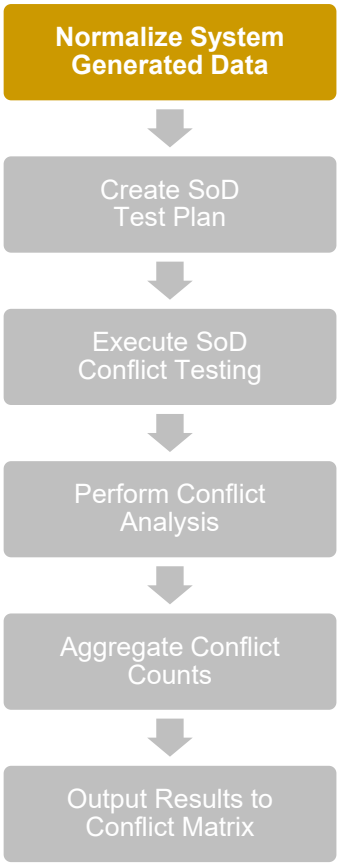


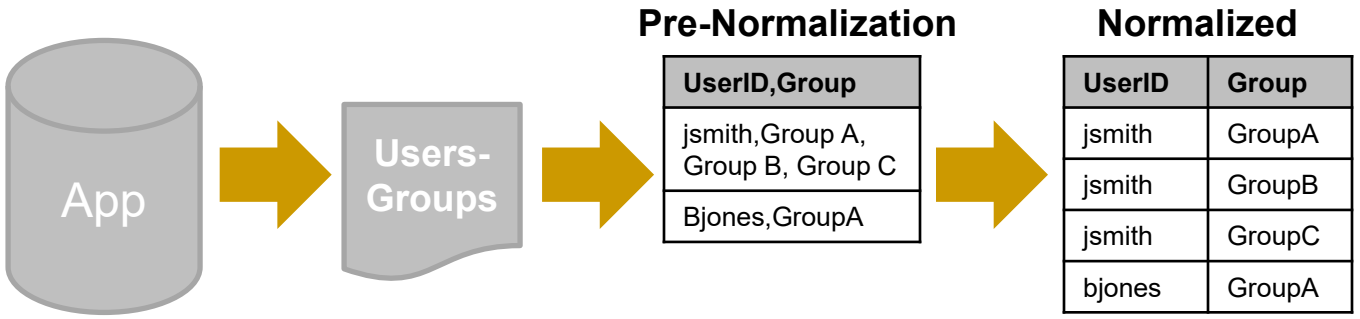
Business Definition | **Technical Definition** | Testing | Mitigation | Remediation

Trust in, and value from, information systems

Normalize System Generated Data

- 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





ISACA®
Trust in, and value from, information systems

Create SoD Test Plan

- 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

Normalize System Generated Data

Create SoD Test Plan

Execute SoD Conflict Testing

Perform Conflict Analysis

Aggregate Conflict Counts

Output Results to Conflict Matrix

SoD Test Plan

ID	E			Application 1	Business Process #2	SOD #2	Sensitive Transaction 2	Application 2
1	Sal		ricing					
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		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	

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

Execute SoD Conflict Testing

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

Normalize System Generated Data

Create SoD Test Plan

Execute SoD Conflict Testing

Perform Conflict Analysis

Aggregate Conflict Counts

Output Results to Conflict Matrix

SoD Test Plan

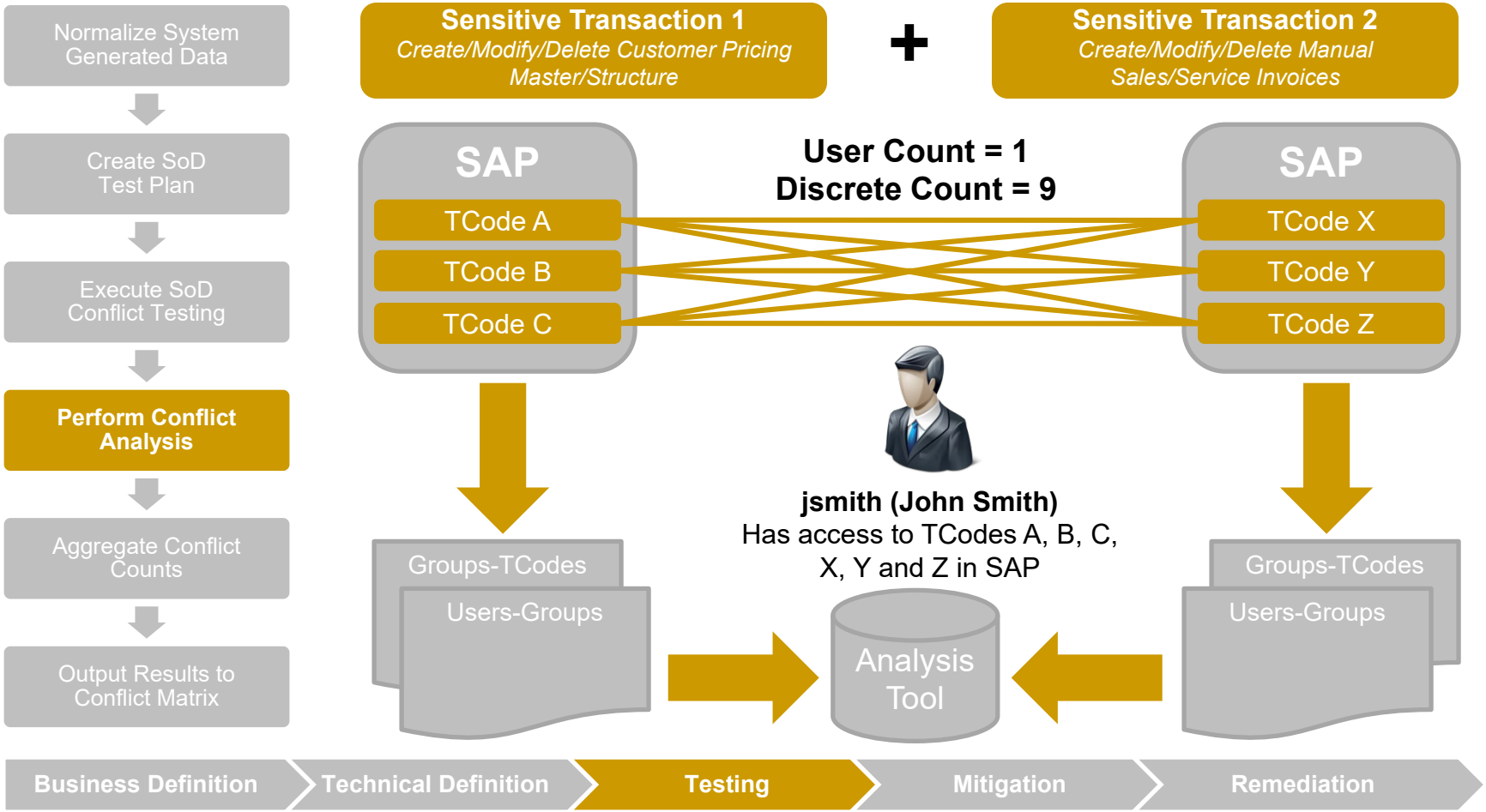
Discrete Conflicts	User Conflicts	Role Conflicts
27,840	4	-
-	-	-
1,214,886	87	24

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

Trust in, and value from, information systems

Perform Conflict Analysis

- Example: Intra-Application Analysis



Trust in, and value from, information systems

Perform Conflict Analysis (Cont.)

- Example: Cross Application Analysis

Normalize System Generated Data

Create SoD Test Plan

Execute SoD Conflict Testing

Perform Conflict Analysis

Aggregate Conflict Counts

Output Results to Conflict Matrix

Sensitive Transaction 1
Create/Modify/Delete Customer Pricing Master/Structure

+

Sensitive Transaction 2
Create/Modify/Delete Manual Sales/Service Invoices

SAP
- TCode A
- TCode B
- TCode C

User Count = 1
Discrete Count = 9

Oracle
- Function X
- Function Y
- Function Z

jsmith (John Smith)
Has access to TCodes A, B, C in SAP and Functions X, Y and Z in Oracle

Groups-TCodes
Users-Groups

Analysis Tool

Resp-Functions
Users-Responsibilities

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

Trust in, and value from, information systems

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

Output Results to Conflict Matrix

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

Normalize System Generated Data

Create SoD Test Plan

Execute SoD Conflict Testing

Perform Conflict Analysis

Aggregate Conflict Counts

Output Results to Conflict Matrix

SoD Test Plan

ID				Application 1	Business Process #2	SOD #2	Sensitive Transaction 2	Application 2	Discrete Conflicts	User Conflicts	Rule Conflicts
					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/Modi Master/Struc								-
5	Sales & Receivables	1	Create/Modi Master/Struc								-
6	Sales & Receivables	1	Create/Modi Master/Struc								1
7	Sales & Receivables	1	Create/Modi Master/Struc								-
8	Sales & Receivables	1	Create/Modi Master/Struc								-
9	Sales & Receivables	1	Create/Modi Master/Struc								24
10	Sales & Receivables	1	Create/Modi Master/Struc								-
11	Sales & Receivables	1	Create/Modi Master/Struc								-
12	Sales & Receivables	1	Create/Modi 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	9	10				
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

Trust in, and value from, information systems

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

ISACA® Trust in, and value from, information systems

Mitigating Controls Tips

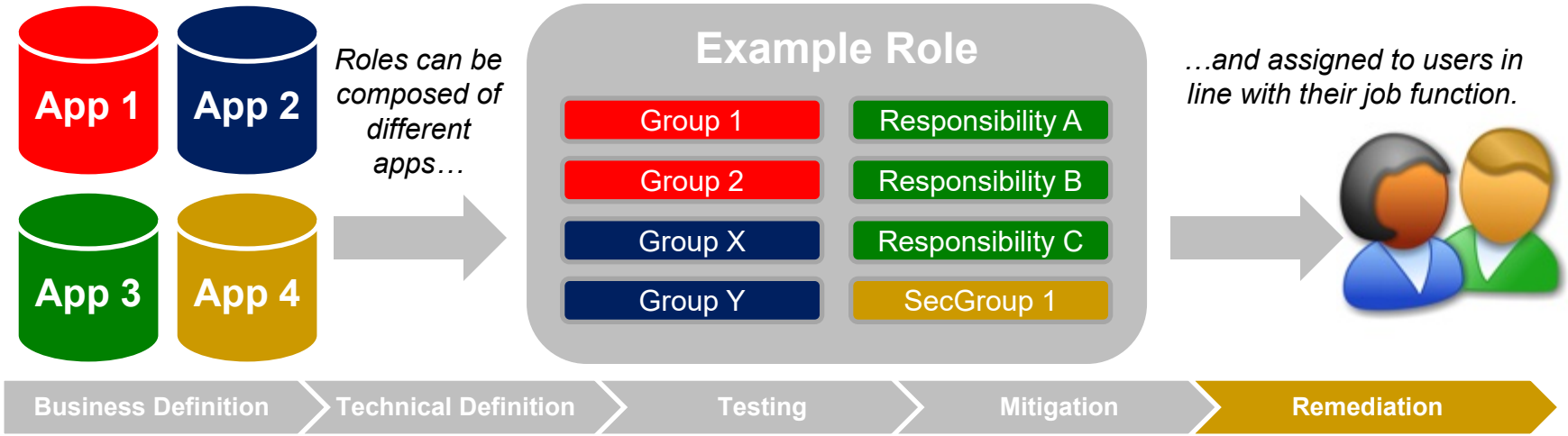
- Mitigating controls must have passed internal audit testing
- Watch for *fox-and-henhouse* conflicts
  - The reviewer and/or approver of the mitigating control cannot be in the conflicted population
  - If this condition exists, the control must either be assigned to someone else to perform or the 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

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



ISACA®
Trust in, and value from, information systems

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

SoD Tools and Applications (continued)

SoD tools and applications can provide:

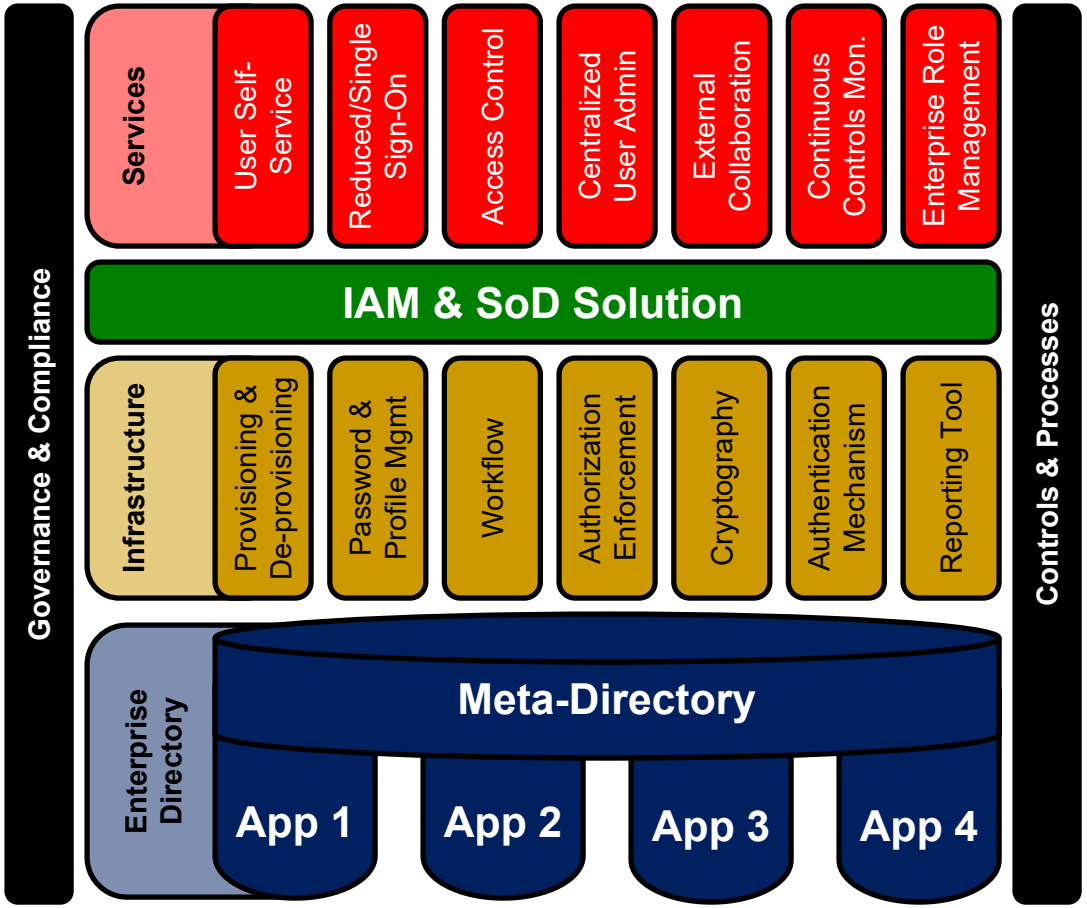
- Better response to internal and external audit requests
- Real-time risk assessment with cross-system analysis
- Large library of SoD rules
- Automated Rules Building
- Automation of mitigating controls
- Reporting options
- Transaction monitoring

Business Definition | Technical Definition | Testing | Mitigation | Remediation

Trust in, and value from, information systems

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

Trust in, and value from, information systems

A Risk-Based Approach to Segregation of Duties

LESSONS LEARNED

Trust in, and value from, information systems

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

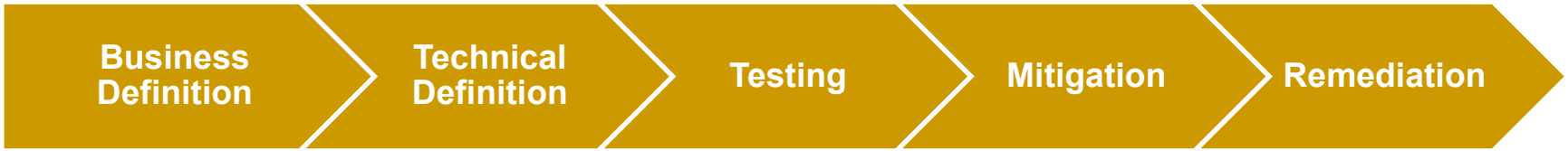
- Accountability is essential: executive sponsorship is required
- The business (finance, accounting, operations, etc.) typically knows the processes the best, but may not understand all the avenues for a potential transaction
- Business is responsible for the business requirements definition; IT enforces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

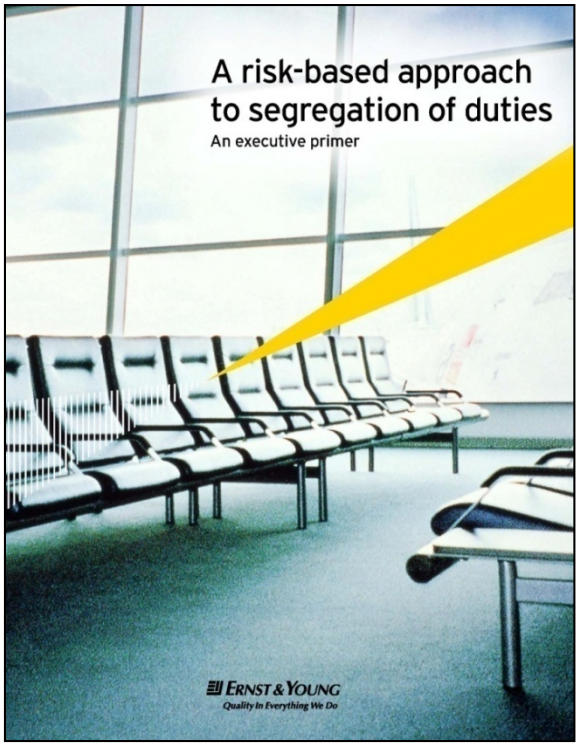


- Proper ownership and governance is essential
- A risk-based approach can accommodate most any sized organization
- Mitigation is an effective risk-management technique
- Remediation can be flexible and suited to the organization's needs and priorities
- Compliance is possible with planning, communication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

Trust in, and value from, information systems

More Information



- SoD Executive Primer/Whitepaper
- Available for download on CFO.com: http://www.cfo.com/whitepapers/index.cfm/displaywhitepaper/12833114?f=search

- SoD Executive Summary
- Available for download at EY.com

ISACA®
Trust in, and value from, information systems

More Information

- Additional useful session - Track 4 – Emerging Issues and ISACA Research
  - Session 244 – How to manage segregation of duties in and SAP environment – Prateek Jain, E&Y
    - Understand the basic SAP security concept
    - Explain the SoD concept
    - Analyze SAP security complexity and how SoD tools help manage SoD issues
    - Assess SoD using SAP GRC business solutions

Trust in, and value from, information systems

Contact Information

Michael Adolphson

Senior Manager
Advisory Practice
Chicago, Illinois

- Michael.Adolphson@ey.com
- Office: (312) 879-3769
- Mobile: (630) 452-5340

Justin Greis

Manager
Advisory Practice
Chicago, Illinois

- Justin.Greis@ey.com
- Office: (312) 879-2266
- Mobile: (312) 342-4202

Thank You

ISACA®
2010 North America CACS
Conference Session

Trust in, and value from, information systems