

# SOD Enterprise Management

ISACA – 9/29/06

# Contents

- **Background / Overview**
  - Segregation of Duties (SOD) Defined
  - Compliance Shift
  - Current-state Observations
  - SOD Enterprise Management
- **Organizational Control**
  - Internal Control Strategy
  - SOD Control Integration
- **Approach**
  - Objectives
  - Phased Approach
  - Sample Timeline
  - Roles / Responsibilities
- **Technology**
  - Overview
  - Demonstration
- **Next Steps**
  - Road Map
- **Questions & Answers**

# SOD Defined

- Segregation of Duties is the separation of tasks between different staff members in order to reduce the potential for financial error and/or fraud. An example of an inappropriate segregation of duties is the ability to process A/R invoices and process cash. If these activities are given to one user, it presents the potential for a misappropriation of funds. From an IT perspective, Systems Development staff should not be allowed to transact within live operations.
- In terms of internal controls, SOD is a large part of the Logical Access component of IT General Computer Controls, and a critical business process control across the organizations.
- The expansion of SOD into a comprehensive top-down EM-SOD strategy provides effective control over your environment, while maintaining an appropriate cost balance.

# Compliance Shift

- SOD has always been a focus for the Accounting Industry, and considered a significant internal control for businesses, but it has not been a necessity for compliance purposes
  - Lack of understanding of SOD within organization
  - Heavy reliance on detect / stand-alone controls
  - Non-standard, decentralized, manual procedures
  - No depth to control operation
- As part of Sarbanes-Oxley and PCAOB Auditing Standard No. 2, effective SOD has become a significant compliance requirement
  - Included as evaluation criteria for Management's Assessment and as an example of a stand-alone significant deficiency
  - Significant factor in Fraud evaluation
  - Key application control for most significant accounts / processes
- Organizations realizing the daunting task of implementing SOD to meet "baseline" compliance standards and address real risk to organization
  - What is the "Baseline"?
  - How do I balance cost with level of control?

# Current-state Observations

- Scope
  - Too much (operationally), yet not enough (compliance)
  - High cost for security management operation / periodic access reviews
- Operation
  - Inability to produce adequate SOD reports
  - Inability to complete access reviews in timely manner
  - Business inability to make informed decisions due to “security translation” issue
  - Incorrect / Inadequate personnel involved in control operation
- Compliance
  - Inability to remediate issues / mitigate risk
  - Excessive audit effort in assessment / validation of logical access controls
  - User Access / SOD Compliance Issues

# SOD Enterprise Management

## **Business Problem:**

Business and IT User Access not effectively analyzed for SOD conflicts / inappropriate access, leading to increased risk of fraud and/or financial misstatement. In the cases where SOD control activities are effectively designed and operated, organizations often experience high costs of operation and compliance.

## **Solution Highlights:**

A top-down risk mitigation strategy supported by the integration and standardization of access security. Common tools and processes are designed to integrate logical access control activities, including segregation of duties.

## **Value Proposition:**

- ✓ Business owners – standardized process/tools to assess/remediate business access issues across enterprise.
- ✓ IT owners – centralized repository, multiple system coverage, standardized process with automated workflow management
- ✓ Overall benefits – more effective control design, reduced cost of compliance, streamlined internal and external audit testing



# Organizational Control Methodology

# Risk Mitigation Strategy

## Keep Us Out of Trouble

## Make Our Business Better

Growing Number of Restatements

Bigger Fines and Settlements

Coordinated Risk Activities

Enhanced Business Processes

Expanding Regulation

Stiffer Sanctions

Optimized Controls

Effective Use of Technology

Catastrophic Reputational Consequences

Criminal Indictments

Improved Risk Reporting and Disclosure

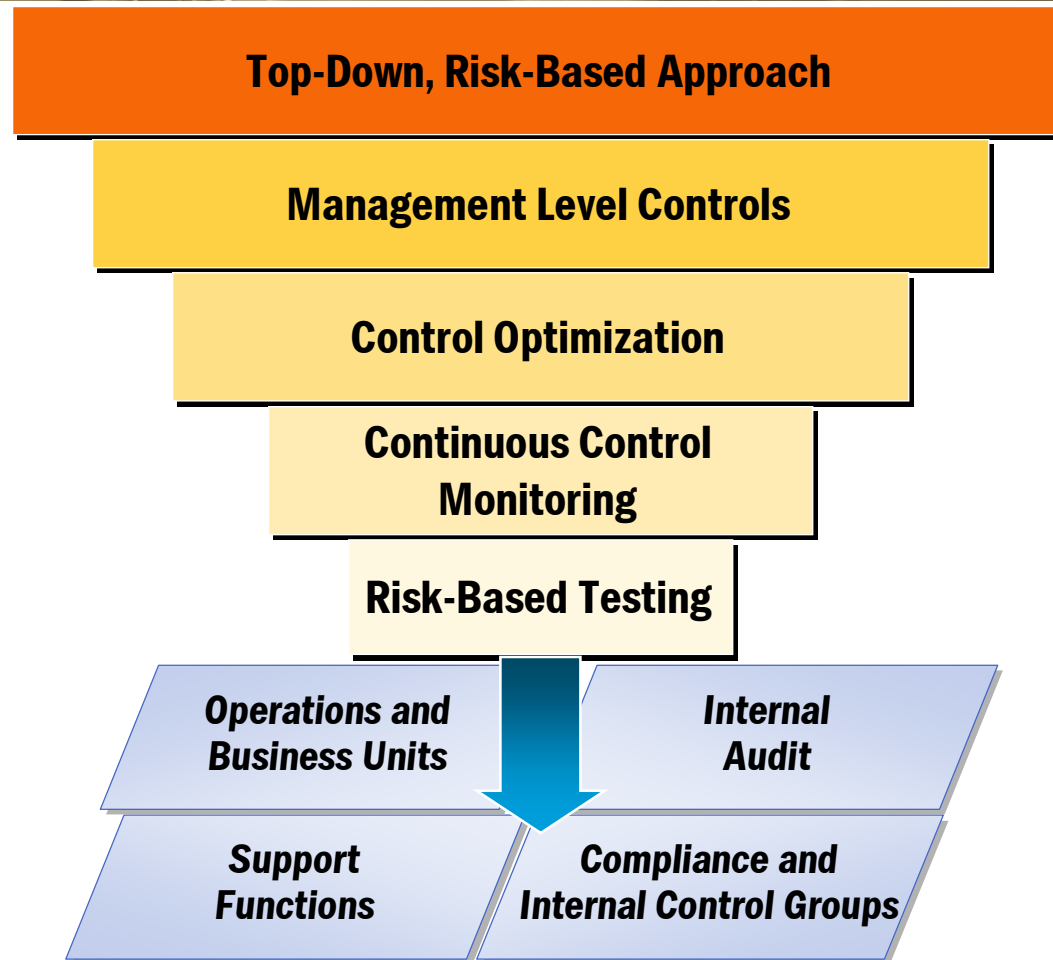
Reduced Total Risk Spend

goal

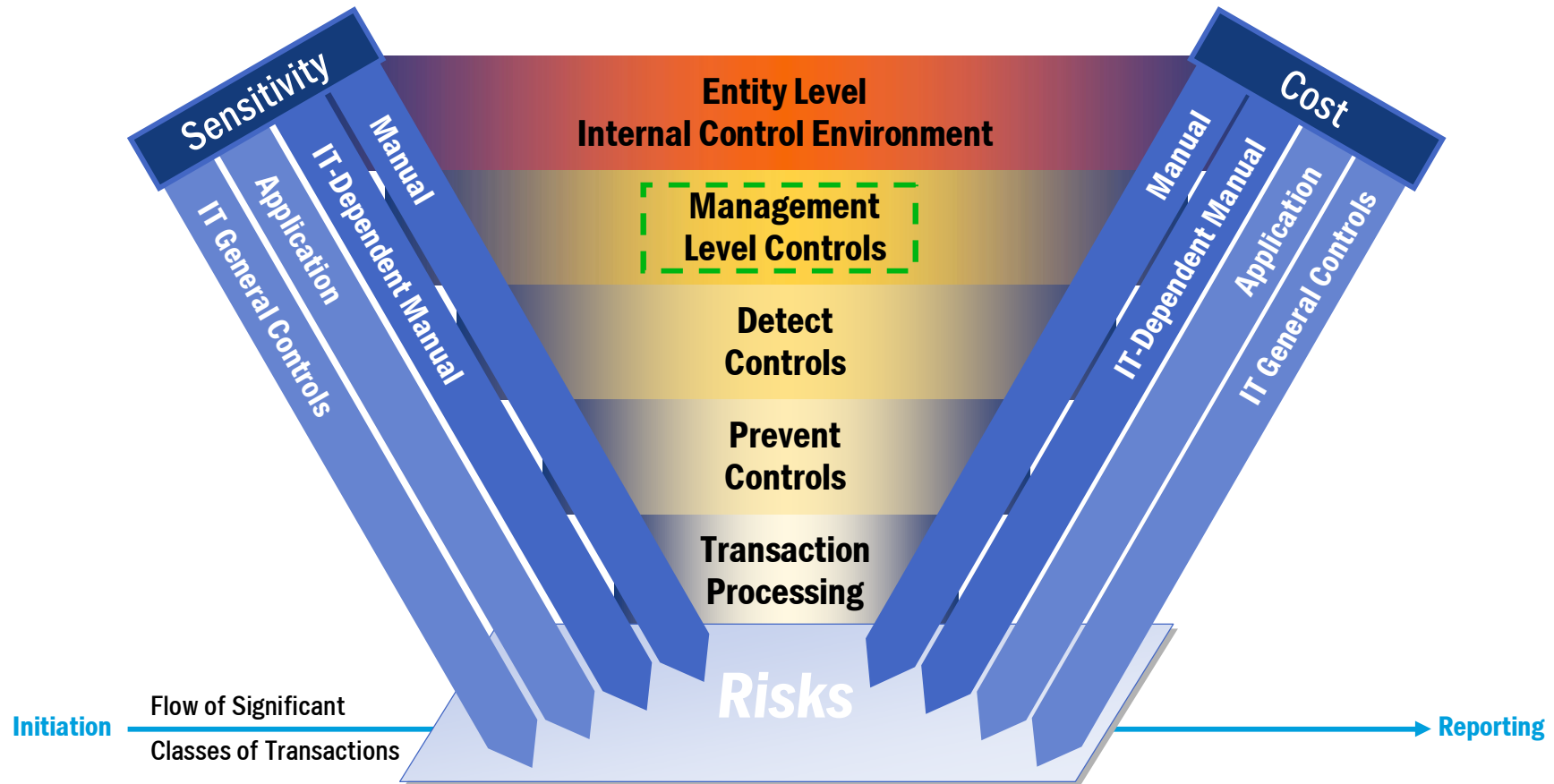
All too confusing and overdone...  
**Except when we get in trouble**

Must do it...  
**But how do we do it better?**

# 404 Project to Process Journey Where Are You?



# Balancing Risks, Controls and Costs



# Continuous Control Monitoring Overview

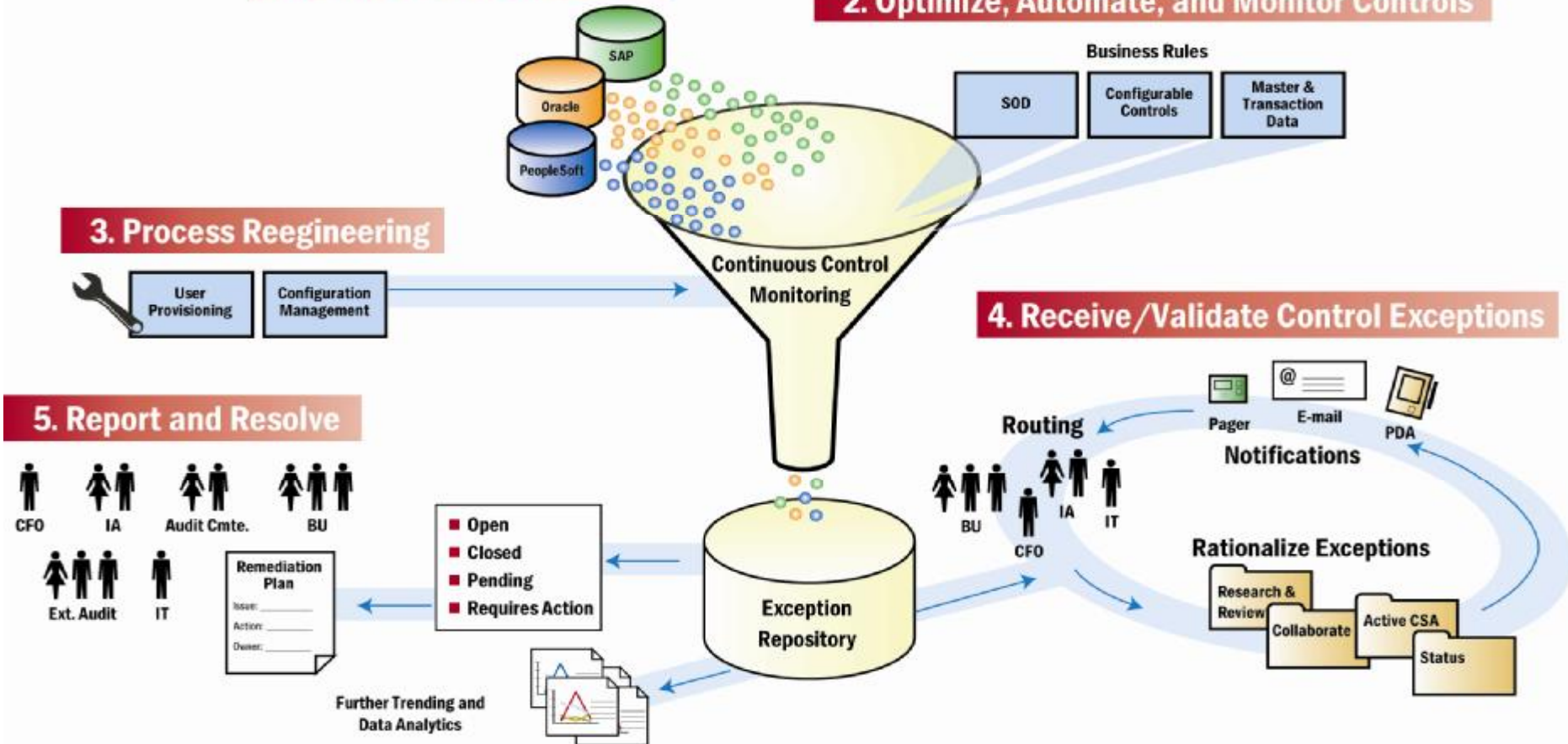
## 1. Connect Data Sources

## 2. Optimize, Automate, and Monitor Controls

## 3. Process Reengineering

## 4. Receive/Validate Control Exceptions

## 5. Report and Resolve



# SOD Control Integration - Sample

- **Evaluate the risk mitigation strategy of your organization**
  - Movement away from pure compliance to better business operation at a lower cost
- **Where is your SOD risk?**
  - Tiered (Scoped) locations / processes / applications according to risk and materiality
- **What Management level controls can be implemented to address SOD risk?**
  - Common processes for Periodic Access Review and Access Administration (Tier 1 applications)
- **How do I optimize my SOD control framework and still achieve control objectives?**
  - Given the CCM strategy and SOD Prevent control for Tier 1, is a periodic review necessary?
  - QAD in Mexico (Tier 3) has limited personnel, so compensating controls will be relied upon
- **Design / Develop / Implement processes and tools for operating controls**
- **Establish procedure for periodically monitoring operation of SOD controls**
  - A monthly report will be generated for monitoring Tier 1 SOD conflicts



# Approach



# Objectives

- Integration, standardization, and automation of user security using common tools and processes. Depending on your specific needs, EM-SOD may include one or all of the following control activities.
  - User provisioning
  - Account management
  - Access management
  - Periodic access reviews
  - Segregation of duties analysis and reviews
  - User de-provisioning
  - Monitoring and reporting
  - System security configurations

# Phased Approach

- **Project Definition / Requirements Gathering**
  - *Output:* Scope, Control Tiers, Current-state Control Analysis, Control Requirements
- **SOD Control Methodology**
  - *Output:* Operative Org Structure , Policies/Business Rules, Entity-level Controls, SOD Rules, Sensitive/Restricted/Prohibited Transactions, Compensating Control Mapping, Maintenance Procedures
- **Tactical Remediation**
  - *Output:* Security Profiles, Transaction Mapping, Conflict Baseline, Access Remediation (Selective)
- **Control Design**
  - *Output:* Control Framework Updates, Control Activity Process Flows / Procedures / Roles and Responsibilities, End-user Training, Automation Requirements
- **Automation Enablement**
  - *Output:* Technology Gap Analysis, Automation Alternatives, Access Management / SOD Tools
- **Control Deployment / Operation**
  - *Output:* Deployment Workplan, Test Plans / Scripts, Operational Output, Monitoring Reports
- **Control Validation**
  - *Output:* Test Procedures, SOD Compensating Controls Monitoring Procedure, Remediation Plans



# Roles / Responsibilities

- SOD Control Owner(s)
  - Coordinate scoping, design and deployment activities (year 1)
  - Coordinate sustainable SOD control operation including CCM (on-going)
- Access Approvers
  - Assist in control / tool design and testing (year 1)
  - Validate appropriateness / SOD validation as part of access administration and periodic reviews (on-going)
- SOD Tool Administrator
  - Assist in implementation of SOD tools (year 1)
  - Maintain operation of SOD tool; support control operation as necessary (on-going)
- IT Administrators
  - Assist in security profiles development and transaction mapping (year 1)
  - Support system changes resulting from control operation (on-going)
- Compliance Team
  - Design/update control framework (given SOD risk mitigation strategy) and associated procedures (on-going)
  - Perform management testing and coordinate with external auditors on integrated approach



# Technology

# E&Y SOD Tools

E&Y SOD tools are the result of quick response solutions to client needs. Although our tools have similar features to market leader software developers, we do not view ourselves as competitors. We try to complement third party tools by filling a particular need, which often times is the client desire to have something immediately. SODA began due to a request to perform cross-system SOD analysis; iSMART was developed for a client who requested a User Provisioning solution and a customized User Access Review interface. Both provided niche features, in addition to being low-cost and fulfilling an immediate need. Keep in mind that a tool is only an enabler, which will provide little to no value without effective control design, control operation, control sustainability and continuous control monitoring.

- **SODA / iSMART**
  - **Fulfills needs for periodic access reviews, segregation of duties reviews, and “what-if” analyses in access administration**
  - **Monitoring and reporting**
  - **Adaptable to ERP’s and in-house systems (mainframe and distributed)**
  - **Cross-system capable**
  - **Assessment & Remediation Tracking**
  - **Centralized Testing Documentation / Support**
  - **User provisioning**
  - **Workflow management**

# SOD Tools Comparison

	SODA (E&Y)	iSMART (E&Y)	Virsa
Customizations	X	X	
Custom reporting	X	X	X
SOD rule customization	X	X	X
"Drill-down" detail	X	X	X
Workflow management		X	X
User Provisioning		X	X
Cross-system analysis	X	X	X
Real-time sensitive transaction code monitoring			X
User risk analysis by position, geographic location, etc.			X
Access review interface	X	X	X
Compensating controls mapping	X	X	X
Compensating control mgt. and workflow			X
"What-If" SOD conflict prevention	X	X	X
Technical Support (Post-Implementation)			X



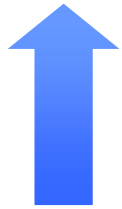
# Next Steps

# Strategic SOD Roadmap

**Strategic**

**Immediate Business Value**

**SOX Compliance**



- Automated audit/compliance testing
- Implement reduced sign-on
- Develop BU & application role models
- Integrate EM-SOD considerations into SDLC

- Enable portal personalization based on role (enabling targeted communications)
- Expand solution to remaining enterprise environments

- Develop EM-SOD enterprise architecture
- Develop enterprise role model
- Leverage AD investment to implement enterprise identity master record source
- Implement automated user provisioning/de-provisioning solution for “material applications”

- Leverage investment to implement automated approval processes
- Develop and implement data classification scheme
- Implement self-service registration and improve password reset capabilities

- Develop and implement EM-SOD policies, standards, & guidelines
- Develop governance & compliance model for managing access
- Review, cleanup, & lockdown account access

- Re-design and implement EM-SOD processes and procedures and validate key controls
- Document and execute management Testing



# Questions & Answers

# Questions



Thank You

Andy Tanner  
Detroit Office  
(248) 457-3876  
[andrew.tanner@ey.com](mailto:andrew.tanner@ey.com)

Chad Kimball  
Louisville Office  
(502) 585-6408  
[chad.kimball@ey.com](mailto:chad.kimball@ey.com)