

Challenges auditing SoD in SAP

20 August 2008

 **ERNST & YOUNG**
Quality In Everything We Do

“Disclaimers”

- ▶ This session is designed to be an interactive dialog to discuss issues commonly encountered during the execution or review of Separation of Duties procedures
- ▶ The objective of this session is to communicate some additional strategies or procedures that may be considered during execution of a Separation of Duties review
- ▶ This session is NOT designed to convey a standard methodology for executing a Separation of Duties review

Agenda

- ▶ Scope of Separation of Duties Analysis
- ▶ Use of Tools
- ▶ Reporting your Results
- ▶ Other Common Issues
- ▶ Other Recommendations
- ▶ Questions

Separation of Duties Scope: Issues

- ▶ Scope and purpose is not clearly defined
 - ▶ SOX / Financial Relevant / Human Resources / Sensitive Data
 - ▶ Process based or Application based review?
 - ▶ SAP alone or SAP & supporting applications

- ▶ Key stakeholders are not involved up front
 - ▶ May limit the ability for others to rely on your work

- ▶ Mitigating Controls
 - ▶ Not tested as part of SoD analysis

- ▶ Risk Acceptance
 - ▶ Typically hard to find documentation of the acceptance of SoD risk

SoD Scope: Recommendations

- ▶ Clearly define your scope
 - ▶ Both “in-scope” and “out-of-scope” items
 - ▶ Define any “exclusions” from your audit
- ▶ Involve External Audit in your scoping exercise
- ▶ Document and **test** mitigating controls
- ▶ Document the acceptance of unmitigated risk

Usage of Tools: Issues

- ▶ Used “as-is delivered”
- ▶ Tool Capabilities
 - ▶ Some tools/versions can only compare at the tcode level
- ▶ Missing Transactions
 - ▶ Multiple tcodes for same function, not all included in analysis
- ▶ Custom Transaction codes
 - ▶ What do they actually do?
- ▶ Industry Solution Transaction Codes
 - ▶ Have they been considered?
- ▶ Rulesets get stale
- ▶ Non-SAP access is not considered
- ▶ Access to the tool is not granted to all stakeholders

Usage of Tools: Recommendations

- ▶ Customize your rulesets
 - ▶ Include all relevant modifications up front
 - ▶ Restrict the ruleset to an agreed upon subset of higher risk conflicts
 - ▶ Enable a process to keep rulesets current
- ▶ Review Custom Programs
 - ▶ Determine if they pose a potential risk
 - ▶ Determine if tcodes are assigned
- ▶ Include Custom Transaction codes in your rulesets
 - ▶ Retain documentation of the analysis to determine which are relevant
- ▶ Review rulesets annually or with any major upgrade
- ▶ Don't rely on the tool alone
 - ▶ Some validation of your results is recommended
- ▶ Provide access to key stakeholders
 - ▶ Don't forget the training!

Reporting your Results: Issues

- ▶ Results are not actionable
 - ▶ Results are not communicated to the necessary stakeholders
 - ▶ Suggested improvements are not included or sufficient in detail

- ▶ Mitigation is too easily accepted
 - ▶ Why mitigate if you can eliminate
 - ▶ Mitigation = long-term cost
 - ▶ Elimination = one-time cost

Reporting your Results: Recommendations

- ▶ Go beyond “Assess” and suggest “Improve” actions
- ▶ Include target dates for completion and track progress
- ▶ Examples:
 - ▶ Review transaction usage
 - ▶ Recommend removal of unused “High” risk transactions from Production roles
 - ▶ Review existing user / role structure
 - ▶ Recommend Tactical role redesign suggestions
 - ▶ Recommend periodic user appropriateness reviews
 - ▶ Recommend elimination of wildcard (*) access
- ▶ At minimum, define your long-term strategy to get clean

Other Common Issues

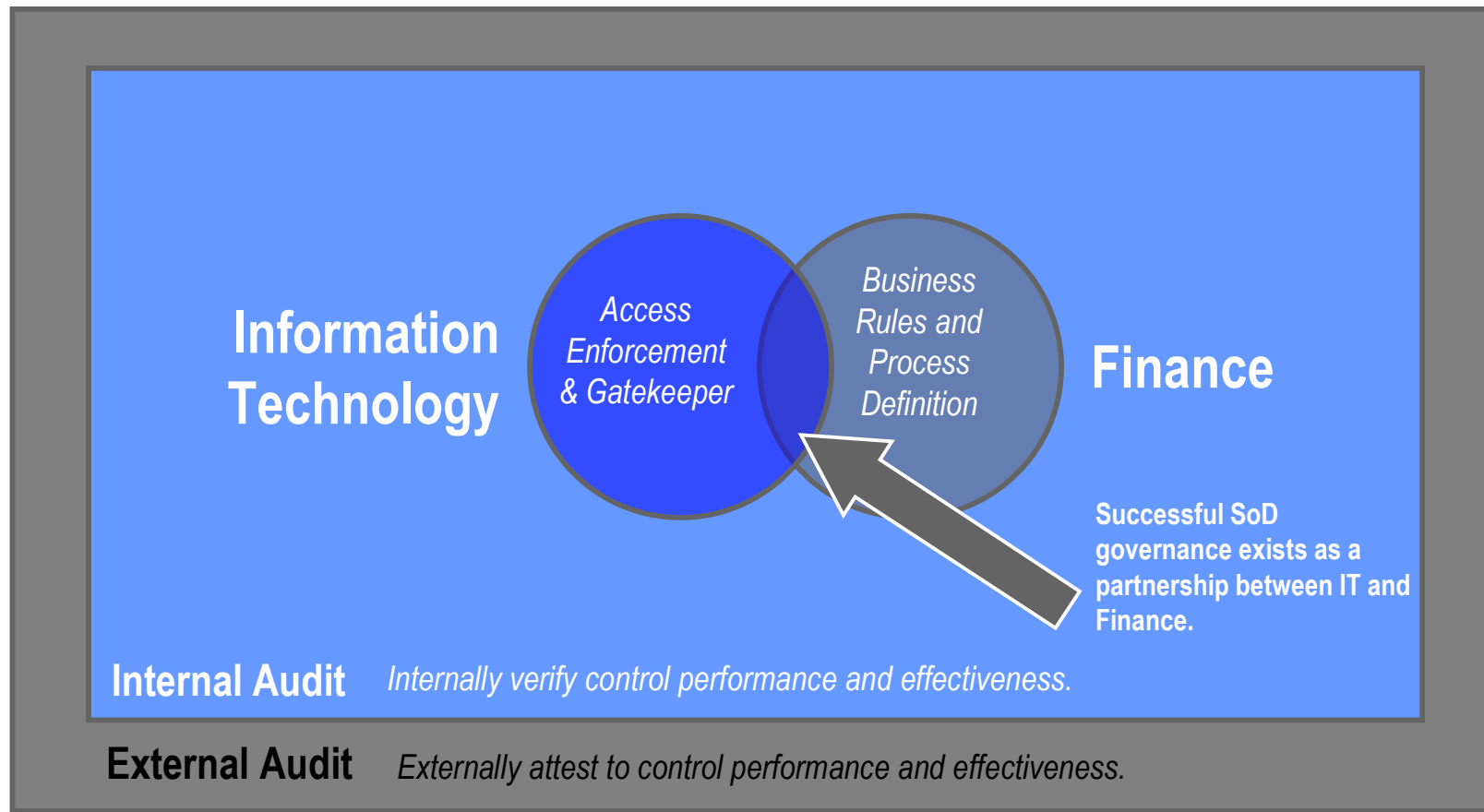
- ▶ Lack of appropriate tools or skills
 - ▶ Manual tracking and reporting is too labor intensive
- ▶ SoD is an afterthought in new SAP implementations
 - ▶ Lack of integration through the blueprint & realization phases
- ▶ Point-in-time SoD Analysis vs. continuous compliance
- ▶ Lack of connection to SoD in user provisioning cycle
- ▶ No connectivity to custom program development process
- ▶ Global rulesets are applied differently in local geographies
- ▶ Ownership is not clearly defined
 - ▶ Viewed as an IT Tool/Process
 - ▶ Viewed as an Auditor Tool/Process

Other Recommendations

- ▶ Define who owns SoD
 - ▶ One Perspective:
 - ▶ Information Technology Dept. is an enabler or facilitator, not owner
 - ▶ Internal Audit can be an owner or facilitator
 - ▶ Business Owners / Finance ultimately own SoD since they accept any residual risk

- ▶ Consider a risk-based approach to your SoD analysis
 - ▶ Focus time on transactions that pose the greatest risk the organization
 - ▶ Risk can be tuned to achieve SoD program objectives (detect fraud, detect material impact to FS, enforce monitoring controls, etc.)
 - ▶ Will focus testing and remediation efforts of the team
 - ▶ Don't try to "boil the ocean"

SoD Ownership & Governance



Question & Answer Session

Contact Information

- ▶ David L. Baumgartner
 - ▶ Ernst & Young, Advisory Services
 - ▶ David.Baumgartner1@ey.com
 - ▶ Office: 612.371.8980