S33 - Segregation of Duties
Scott Mitchell and Colin Wallace
Segregation of Duties
Scott Mitchell, Senior Manager (503) 478-2193
Colin Wallace, Senior Manager (503) 478-2185

Our Objectives

• Clarify the role of Segregation of Duties (SOD)
• Demonstrate how to implement effective SOD
• Clarify the evaluation process of current user access
• Demonstrate that management is always surprised after evaluating their SOD
Agenda

• Discuss fraud and risks of fraud
• Define SOD
• Demonstrate a method for evaluating SOD
• Considerations for maintaining SOD
• Examples of findings

Fraud examples in the news…

• Societe Generale
  – French bank loses $7.2B due to unauthorized trading
• Siemens AG
  – Fraudulent consulting contracts ($500M)
• NEC
  – Invalid revenue ($18M) and kickbacks ($4.2M)
• NBC Universal, Inc.
  – Treasurer charged with wire fraud ($813K)
The Fraud Triangle

Pressure/Incentive

Opportunity

Rationalization

What is Segregation of Duties?

• How do you define it?

• What is the goal of segregation of duties?

• Are all SOD conflicts equal in importance?
What is Segregation of Duties?

• COSO: “Dividing or allocating tasks among various individuals making it possible to reduce the risks of error and fraud.”

• Contains four components
  – Custody
  – Authorization
  – Record Keeping
  – Reconciliation

What is Segregation of Duties (cont.)?

• Ideally, a single individual would have responsibility for only a single component

• Benefits include:
  – Safeguarding of assets
  – Accurate financial reporting
  – Reduced risk of non-compliance
  – Reduced cost of compliance for automated SOD
    (e.g., SOX and external audit)
What is Segregation of Duties (cont.)?

• SOD conflicts are not equally important to every company:
  – Safeguarding of assets vs. financial reporting risks
  – Relative importance of information confidentiality
  – Reduced risk when the “chain” of access is broken

• SOD risks are company specific

Evaluating Your SOD

• Create a policy
  – Include a statement that management is responsible for enforcing the policy and maintaining proper SOD
  – Ultimately includes a list of incompatible duties

• Identify the core tasks performed at your company
Evaluating Your SOD

• Identify incompatibilities

  – Risk based for your business

  – Consider “sensitive” duties such as posting of journal entries, performing reconciliations and Vendor Master

Example SOD Matrix
Evaluating Your SOD (cont.)

• Translate requirements into applications
  – Define menus or objects granting user access
  – Identify the “sensitive” objects associated with conflicting duties
    • Time consuming depending on the system

Evaluating Your SOD (cont.)

– Roles for key responsibilities with well defined rights
  • Shipping/Receiving
  • Purchasing
  • Accounts Payable
  • Accounts Receivable
  • Vendor Master
### Evaluating Your SOD (cont.)

**Object** | **Description** | **Area**
---|---|---
P0012 | Automatic Accounting Instructions | AAI
P0022 | Tax Rules | Tax
P030G | G/L Bank Accounts | Accounting
P03013 | Customer Master | Customer Master
P03B0001 | Speed Receipts Entry | Receiving
P03B0002 | Invoice Revisions | Vendor Invoices Entry/Edit
P03B102 | Standard Receipt Entry | Receiving
P03B11 | Standard Invoice Entry | Vendor Invoices Entry/Edit
P03B11SI | Speed Invoice Entry | Vendor Invoices Entry/Edit
P03B11Z1 | Batch Invoice Revisions | Vendor Invoices Entry/Edit
P03B121 | Work With Electronic Receipts Input | Receiving
P03B123 | Electronic Receipt Entry | Receiving
P03B305 | Credit Granting / Management | Customer Master
P03B42 | A/R Deduction Activity Master Maintenance | Customer Master

---

### Evaluating Your SOD (cont.)

- Determine the existing role access rights
  - Identify built-in conflicts provided by each role
  - Document desired changes to roles

- Determine the users assigned to roles
  - Provides a complete list of user conflicts allowed
Evaluating Your SOD (cont.)

<table>
<thead>
<tr>
<th>Role</th>
<th>Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GL</td>
<td>P0012</td>
<td>Automatic Accounting Instructions</td>
</tr>
<tr>
<td>GL</td>
<td>P0030G</td>
<td>GL Bank Accounts</td>
</tr>
<tr>
<td>AR</td>
<td>P03813</td>
<td>Customer Master</td>
</tr>
<tr>
<td>AR</td>
<td>P03820</td>
<td>Credit Granting/Management</td>
</tr>
<tr>
<td>AR</td>
<td>P03842</td>
<td>AR Deduction Activity Master Maintenance</td>
</tr>
<tr>
<td>Receiving</td>
<td>P03B001</td>
<td>Speed Receipts Entry</td>
</tr>
<tr>
<td>Receiving</td>
<td>P03B102</td>
<td>Standard Receipt Entry</td>
</tr>
<tr>
<td>Receiving</td>
<td>P03B121</td>
<td>Work With Electronic Receipts Input</td>
</tr>
<tr>
<td>Receiving</td>
<td>P03B123</td>
<td>Electronic Receipt Entry</td>
</tr>
<tr>
<td>Tax</td>
<td>P0022</td>
<td>Tax Rules</td>
</tr>
<tr>
<td>AP</td>
<td>P03B002</td>
<td>Invoice Revisions</td>
</tr>
<tr>
<td>AP</td>
<td>P03B11</td>
<td>Standard Invoice Entry</td>
</tr>
<tr>
<td>AP</td>
<td>P03B11S</td>
<td>Speed Invoice Entry</td>
</tr>
<tr>
<td>AP</td>
<td>P03B12Z1</td>
<td>Batch Invoice Revisions</td>
</tr>
</tbody>
</table>

Tables such as the above will provide information of user access to sensitive transactions

Evaluating Your SOD (cont.)

The above graphic depicts how user conflicts can be identified using lists of:
- Users/roles
- Roles/objects/transaction types
- Conflicting pairs of transaction types
Evaluating Your SOD (cont.)

• Added Requirements
  – Roles should not contain “built-in” conflicts

• Additional issues and complexity
  – Users assigned to multiple roles
  – Users assigned access rights by User ID
  – Users accessing multiple systems

Evaluating Your SOD (cont.)

• Does this solve all issues? Not likely.
  – Small groups of users
  – System constraints
  – Manual activities outside the system

• Detective controls have a role
  – Audit trails
  – Exception reports
Evaluating Your SOD (cont.)

• Other sources of SOD concern:
  – Application administrator access
  – Security administrator and user setup
  – Programmer access to production
  – Powerful utilities
  – Strength of authentication
  – Shared passwords
  – Access to edit / change audit tables

Maintaining SOD

• Prevention
  – Tools for granting user access rights
    • IT becomes a gatekeeper
    • Conflicts raised for added approval or mitigation

  – Role and user change controls

  – Maintain strong authentication requirements
Maintaining SOD (cont.)

• Detection
  – Internal audit
  – Periodic evaluation and monitoring
  – Exception reporting

• Automated Methods
  – Automated monitoring
  – ERP system tools and workflow

SOD Observations

• What have you seen in SOD findings?

• What conflicts are most concerning to you and your company?
Management is Surprised…

• All 51 users in a Lawson implementation could enter and approve journal entries

• 21 users could enter/approve cash receipts, enter/approve journal entries and perform bank reconciliations

Management is Surprised…

• 105 users in a revenue related system could modify user security

• 223 users in a revenue system could modify the cash drawer beginning balance

• 316 users had access to virtually all sensitive transactions in a hospital revenue application
Management is Surprised…

• 3,100 KRONOS users could authorize their own payroll
  – 1,100 were hourly employees who could approve their own overtime
  – All 3,100 could change their vacation accruals and approve payment in-lieu of vacation

Key Points

• Segregation of Duties helps prevent fraud and errors
• Companies should identify their SOD risks and controls
• Detective controls can be effective
• A process is needed to correct ineffective SOD
• Maintaining effective SOD requires processes and tools
• Management is always surprised about current access
• Without performing an analysis, SOD issues are apparent after something bad occurs
Questions and Answers

Thank You!

Scott Mitchell
Scott.Mitchell@mossadams.com
(503) 478-2193

Colin Wallace
Colin.Wallace@mossadams.com
(503) 478-2185

The material appearing in this presentation is for informational purposes only and is not legal or accounting advice. Communication of this information is not intended to create, and receipt does not constitute, a legal relationship, including, but not limited to, an accountant-client relationship. Although these materials may have been prepared by professionals, they should not be used as a substitute for professional services. If legal, accounting, or other professional advice is required, the services of a professional should be sought.