Segregation of Duties

Presented by:
Brian Pye, Principal
Megan Moore, Manager

February 6, 2014

CliftonLarsonAllen

cliftonlarsonallen.com

Learning Objectives

- Understand what segregation of duties is and why it is important
- Understand the relationship of internal control and segregation of duties
- Understand manual vs. technical segregation of duties
- Understand best practices of segregation of duties
- Demonstrate how to implement effective segregation of duties

What is Segregation of Duties?

- COSO Definition: “Dividing or allocating tasks among various individuals making it possible to reduce the risks of error and fraud.”
- The optimal design for internal controls is separating the 4 significant components of a transaction or activity
  - Initiation of transaction or activity
  - Authorization of transaction or activity
  - Recording of transaction or activity
  - Reconciliation of transactions or activities
- Ideally a single individual would have responsibility for only a single component

What is Segregation of Duties?

- SoD conflicts are not equally important to every organization:
  - Safeguarding of assets vs. financial reporting risks
  - Relative importance of information confidentiality
- SoD conflicts are not equally important in every business function
  - Human resources vs. payroll risks
  - Donor marketing/targeting vs. cash receipts
- SoD risks are organization specific
  - Number of resources in a business function
  - Mitigating internal controls

Why is Segregation of Duties Important?

- Benefits include:
  - Safeguarding of assets
  - Accurate financial reporting
  - Reduced risk of errors
  - Reduce cost if SoD is automated and configured into the system
  - Reduce the opportunity of fraudulent activity and unethical behavior

Segregation of Duties Is An Internal Control

- An internal control is a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives
- Effected by people. It is not merely about policy manuals, systems, and forms, but about people at every level of an organization that impact internal control
- Able to provide reasonable assurance, not absolute assurance, to an entity's senior management and board
- Adaptable to size and complexity of an organization

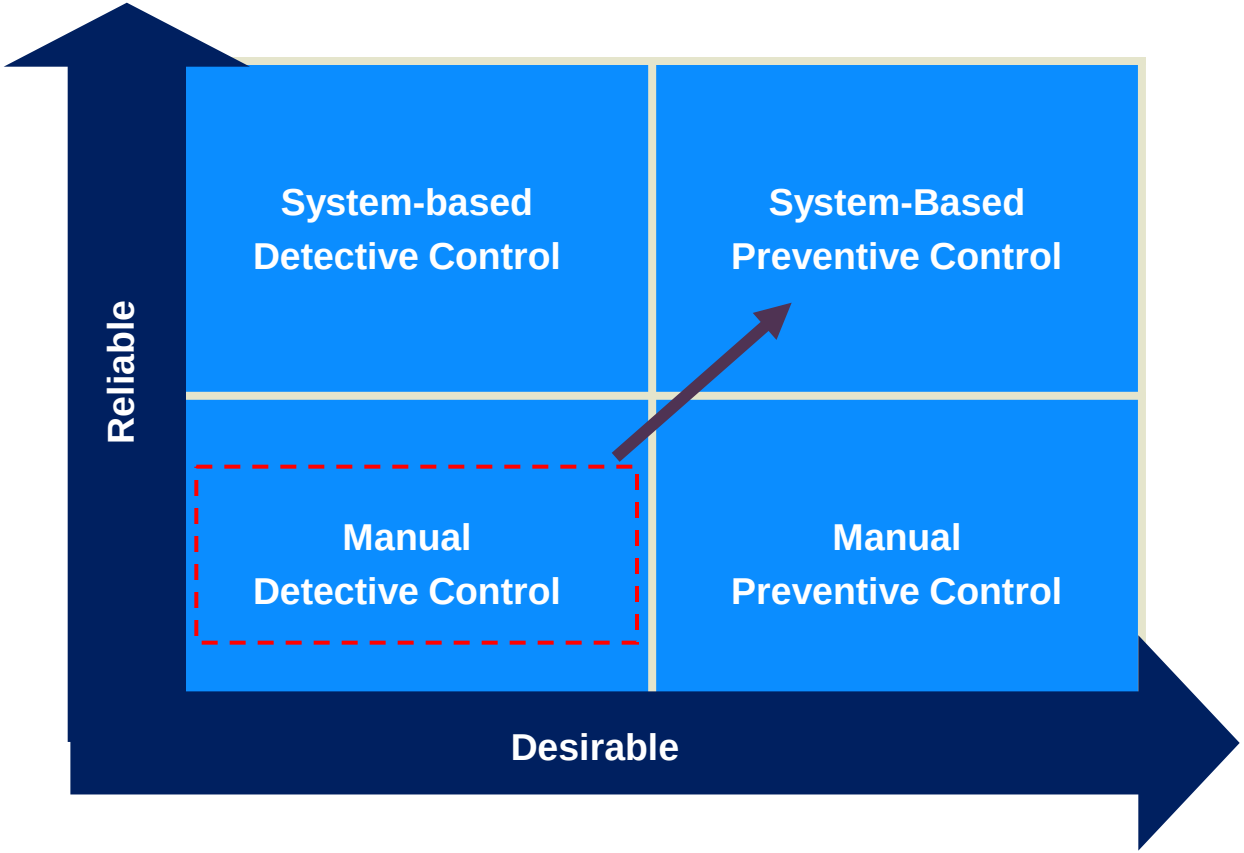
Source: Committee of Sponsoring Organizations of the Treadway Commission (COSO)

Types of Internal Controls

- Automated vs. Manual
  - Manual controls are subject to human error
  - Automated controls can impact large volumes of transactions and apply a standard set of business rules or programmatic logic to each transaction
- Preventative vs. Detective
  - Preventative controls are designed to prevent the occurrence of errors and fraud
  - Detective controls are designed to detect errors and fraud that have already occurred
  - SoD is a preventative internal control

Types of Internal Controls

- Two methods to segregate responsibilities:
  - Manually via people and processes
  - Technically/automated via systems/applications



Manually Segregating Responsibilities

- 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 processes and tasks performed at your foundation.
- Identify incompatibilities
  - Consider “sensitive” duties such as posting of journal entries, performing reconciliations, and setting up vendors in the vendor master file

Examples of SoD Best Practices

- Accounting
  - Initiate journal entries
  - Approve journal entries
  - Post journal entries
- Accounts Payable
  - Create a new vendor in vendor master file
  - Process an invoice
  - Cut AP checks
  - Reconcile AP

Examples of SoD Best Practices

- Accounts Receivable
  - Set up donor in master file
  - Physically receive cash, check, wires, etc.
  - Reconcile cash
- Payroll
  - Create a new employee in payroll master file
  - Process payroll
  - Cut payroll checks
  - Reconcile payroll

Technically Segregating Responsibilities

- Translate policy SoD requirements into applications
  - Setting up using role based permissions
  - Setting up at the end user level
  - Setting up using specific fields
- 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
  - Gather a complete list of users and roles assigned
  - Identify conflicts and issues

Technically Segregating Responsibilities

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

Evaluating SoD at Your Foundation

- Does this solve all issues? Not likely.
  - Lack of resources
  - System constraints
  - Manual activities outside the system
- Detective controls have a role
  - Internal controls to review and approve various transactions performed (manual)
  - Audit trails (technical)
  - Exception reports (technical)

Evaluating SoD at Your Foundation

- Other sources of SoD concern:
  - Application administrator access
  - Security administrator and user setup
  - Programmer access to production
  - Strength of authentication
  - Shared passwords
  - Access to edit / change audit tables

Maintaining SoD

- Prevention
  - Tools for granting user access rights
  - Role and user change controls
  - Maintain strong authentication requirements
- Detection
  - Internal audit
  - Periodic evaluation and monitoring
  - Exception reporting
- SoD is a business and technical issue
  - Involvement by the business functions
  - Involvement by the information technology function

Evaluating SoD at Your Foundation

- What has your foundation done to mitigate the risk of segregation of duties conflicts?
- What type of SoD findings do you recognize or have already been addressed at your foundation?
- What conflicts are most concerning to you and your foundation?

Management is Surprised

- More times than not, management is surprised about how much access individuals are assigned
- Management is surprised at the level of effort that is required by the business functions to implement proper segregation of duties within systems

SoD Implementation Roadmap

- Step 1: Identify all key processes critical to your foundation
- Step 2: Identify all key activities within key processes utilizing criteria described (i.e. initiating, approving, recording, reconciling) and determine which employees are performing those key activities
- Step 3: Determine what activities are already segregated and what activities are not
- Step 4: Redesign processes to segregate additional activities that are not currently segregated
- Step 5: Review SoD in the system and make changes to users system access to align with the policy segregation

SoD Implementation Roadmap, Cont.

- Step 6: Identify activities that cannot be segregated due to size and/or limited resources and identify additional controls to be implemented to mitigate the risk.

Key Points

- Segregation of duties helps prevent fraud and errors
- Foundations should identify their SoD risks and internal controls to mitigate risk
- Detective controls can be effective
- A process is needed to correct ineffective SoD
- Maintaining effective SoD requires processes and tools
- Management is almost always surprised

Brian Pye
Principal
(612)-397-3139
Brian.Pye@claconnect.com

Megan Moore, CIA, CISA, CRMA
Manager
(612)-397-3129
Megan.Moore@claconnect.com