Deloitte.

Segregation of Duties:

404 and Beyond

Dan Hirstein
Director – ERS

Thursday, February 10, 2005

Agenda

- Why is SOD Important???
- 404 and Segregation of Duties
- Segregation of Duties Components
- Common Segregation of Duties Conflicts
- Guide To An Effective Assessment Project
  - Building a Segregation of Duties Matrix
  - Assessment Results
  - Remediation Approach
  - Project Lifecycle
- Questions

Why is SOD Important???

- Definition of Segregation of Duties

  Controls that represent the separation of incompatible business duties and/or responsibilities

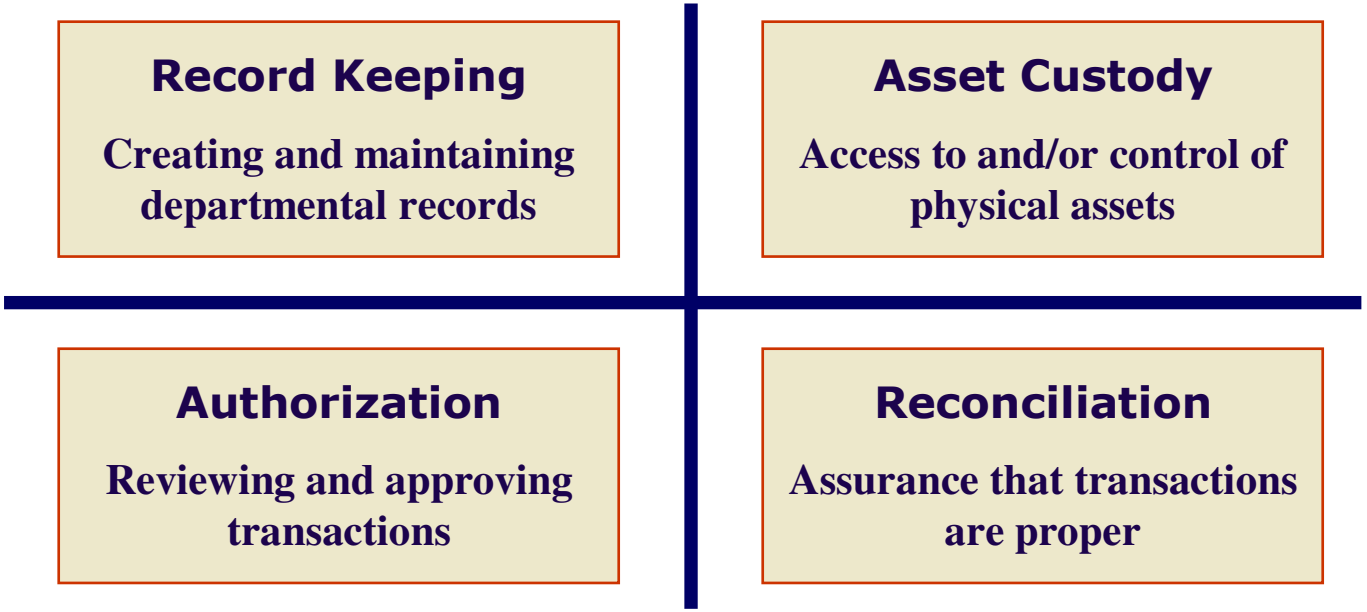
  - Mitigates process risks associated with functional business areas
  - Helps to ensure that one person is not able to:
    - Conceal errors and/or irregularities
    - Cause the inaccurate or incomplete reporting of financial information
    - Commit fraud, theft, or other illegal acts
- Importance
  - Lack of SOD controls can allow for circumvention of business processes
  - Many frauds and corporate scandals can be attributed to poor SOD controls
  - Sarbanes-Oxley regulation specifically states the need for good SOD controls
- Common Misconceptions
  - SOD is only an Information Technology control
  - SOD is only a business unit control
  - Access controls will by nature resolve SOD issues
  - If the company hires good people SOD is not an issue

404 and Segregation of Duties

- Requirements of Management
  - As part of its assessment regarding internal controls, Management must demonstrate that it has contemplated the Segregation of Duties in the design, documentation, and testing of its internal control environment. Specifically mentioned in paragraph 42.
- Requirements of the Auditor
  - In considering Management's assessment regarding internal controls, the Auditor must understand how management contemplated the Segregation of Duties in its 404 compliance program, and the Auditor must test the effectiveness of the Segregation of Duties controls.

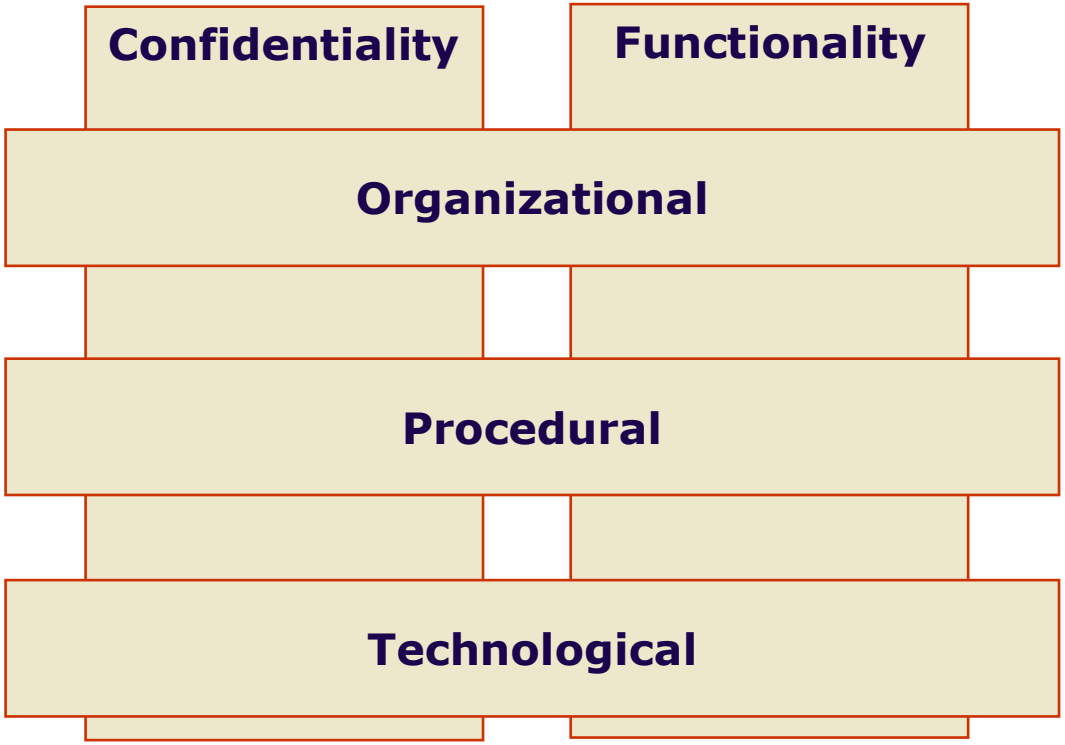
Segregation of Duties Components

- Incompatible Job Functions
  - To maintain proper Segregation of Duties, no employee should be responsible for two or more of the following four functions for a single transaction class.



Segregation of Duties Components

- Dimensions of Segregation of Duties
  - There are several dimensions across which Segregation of Duties can be considered.



Common Segregation of Duties Conflicts

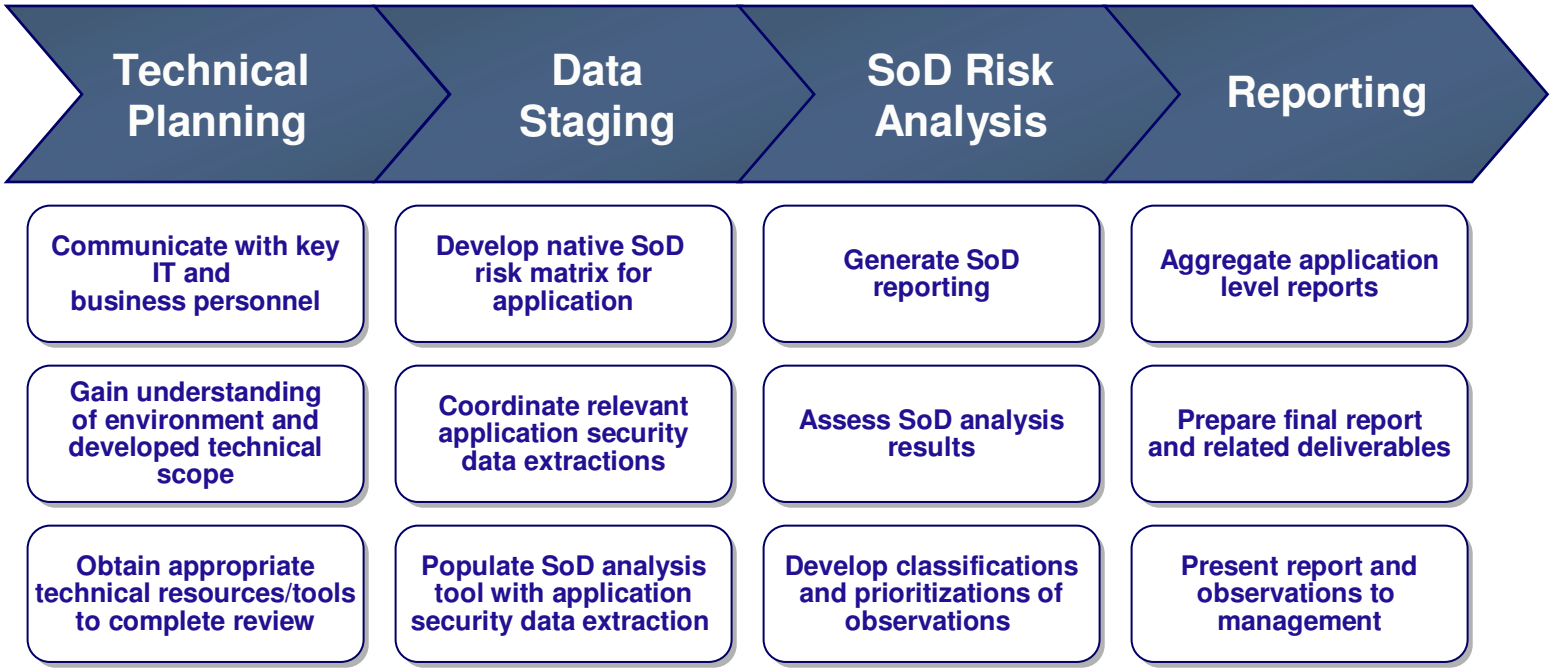
- Information Technology Organization
  - Developers with update access to production data and migration processes
  - Security officers with system administration capabilities
  - ?????
- Process Level
  - Users with ability to add vendors and control payments
  - Payroll and Employee Administration capabilities
  - Input and review performed by same person
  - ????
- Common Causes of SOD Conflicts
  - Lack of understanding of application security
  - Excessive access assigned to user community
  - Lack of management oversite and review
  - Organizational structure
  - ????

Guide To An Effective Assessment Project

- The Challenge
  - The central challenge underlying Segregation of Duties is arriving at a consensus as to what the **rules** should be. Management, Information technology and functional business teams will all have perspectives that should be reconciled in developing the rules that will be followed by an organization.
- The Rules
  - Predefined rules should be the initial focus in any Segregation of Duties project. Management can not assess and the Auditor can not test unless the specific Segregation of Duties rules are clearly articulated.
  - While many organizations have policies and procedures that address Segregation of Duties at a strategic level, relatively few have explicitly stated the detailed Segregation of Duties rules that should be followed at organizational, procedural, and technological levels.
  - There are many ways to express the detail Segregation of Duties rules that an organization will follow. The most common is a Segregation of Duties matrix which lists the key roles and responsibilities within a process or function.
  - Cross-application Segregation of Duties rules should also be considered in environments where there are multiple systems and processes which may conflict.

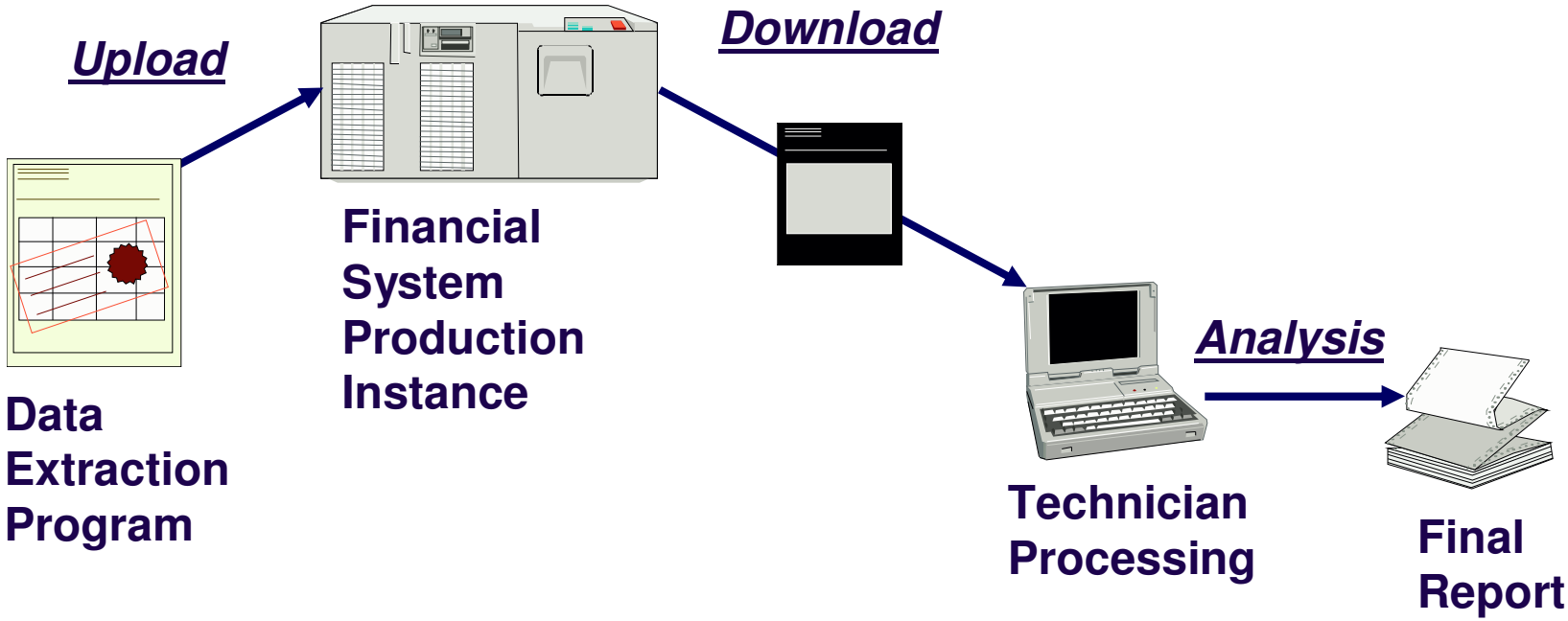
Guide To An Effective Assessment Project

- Management Assessment Approach
  - A clear methodology should be communicated at the beginning of the Segregation of Duties management assessment.



Guide To An Effective Assessment Project

- **Leveraging Technology**
  - Technology should be leveraged in performing the Segregation of Duties assessment. Depending on the tool selected, it may operate directly in conjunction with the production environment being assessed, or it may operate offline on a basis of data extractions.



Segregation of Duties Matrix

				Group	01	02	03	04	05	06	07	08	09	10	11	12
	2	01	****	CUSTOMER MASTER		X	X				X	X	X	X	X	
+	22	02	****	CREDIT MANAGEMENT	X						X		X	X	X	
·	23		F.28	Reset Credit Limit												
·	24		F.34	Credit management mass change												
·	25		FD24	Credit limit changes												
·	26		FD32	Change Customer Credit Management												
·	27		FD37	Credit management mass change												
−	28	03	****	BLOCKED CUSTOMERS	X								X	X	X	
+	31	04	****	PRICING CONDITIONS							X	X	X	X	X	
+	49	05	****	REBATE AGREEMENTS							X	X	X	X	X	
+	54	06	****	CUSTOMER CONTRACTS							X	X	X	X	X	
+	57	07	****	ORDERS	X	X		X	X	X		X	X	X	X	
+	62	08	****	BLOCKED SD DOCUMENTS	X			X	X	X	X		X	X	X	
+	65	09	****	INVOICING	X	X	X	X	X	X	X	X		X	X	
+	69	10	****	A/R PAYMENTS	X	X	X	X	X	X	X	X	X		X	
+	84	11	****	A/R ENTRY - FI	X	X	X	X	X	X	X	X	X	X		
+	88	12	****	VENDOR MASTER - PURCHASING												
+	92	13	****	VENDOR MASTER - ACCOUNTING												
+	96	14	****	VENDOR MASTER - CENTRAL												
+	100	15	****	BLOCKED VENDORS - PURCHASING												X
+	102	16	****	BLOCKED VENDORS - ACCOUNTING												X
+	104	17	****	BLOCKED VENDORS - CENTRAL												X
+	106	18	****	A/P VOUCHER ENTRY												X
+	114	19	****	BLOCKED VENDOR INVOICES												X
+	116	20	****	A/P ENTRY - FI												X
+	121	21	****	A/P PAYMENTS												X
+	143	22	****	BANKING MASTER DATA												
+	148	23	****	CHECKS MANAGEMENT											X	
+	161	24	****	MATERIAL / SERVICE MASTER												
+	165	25	****	DELIVERY / POST GOODS ISSUE	X	X	X	X	X	X	X	X	X	X	X	
+	169	26	****	SHIPMENTS	X	X	X	X	X	X	X	X	X	X	X	

- Segregation of Duties Matrix
  - Transactions (or panels, screens, etc.) and related objects are arranged into logical groups.
    - Called a "Report Group"
  - Groups can be customized to include custom or previously unidentified transactions.
    - The input is a success factor
  - Related groups are clustered for evaluation.
    - Called a "Business Cycle"
  - Groups are represented in a two-dimensional array
    - An 'X' at the intersection of two groups denotes a logical SoD conflict
    - Called a "Conflict Group"
  - Risk levels are attributed to each conflict group to facilitate prioritization
    - Low, Medium, High

Segregation of Duties Matrix

- Key Factors to Consider
  - No single matrix will fit every organization. Use pre-existing material as a starting point, and understand that it will need to be customized to your organization.
  - Developing a consensus regarding the rules is essential. Involve Management and functional business teams, and later the Auditor.
  - The final rules that are developed should reflect the realities of the organization. The rules should hold the functional business teams to a standard but also be reasonable. The process should not prevent the business from functioning.
  - Internal workshops have proven to be an effective tool for educating Management and functional business teams, and in developing the required consensus regarding the rules that will be used.
- Workshop Goals
  - To communicate with functional business teams regarding the organization's approach to assessing risks associated with Segregation of Duties weaknesses
  - To solicit feedback from functional business teams regarding the draft matrix and any feasible changes that should be considered
  - To present tentative observations regarding the status of Segregation of Duties within functional business areas

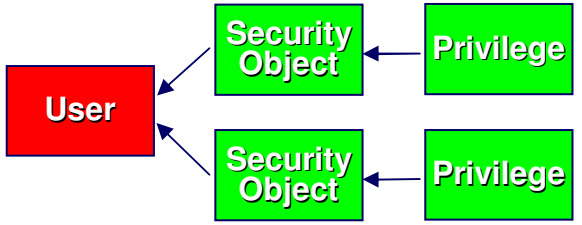
Segregation of Duties Matrix

- Conflict Types
  - In the context of the technological component of the functionality thread of Segregation of Duties, there are two types conflicts.
    - Conflicts that arise from a role (e.g. user profile) being defined with excessive, conflicting privileges (intra-conflicts)
    - Conflicts that arise from multiple security roles being assigned to a user account such that the cumulative privileges of the user are excessive and conflicting (extra-conflicts)

- Intra-Conflicts

  - The conflicting privileges introduce risk when assigned to a user through a single security object.

- Extra-Conflicts



  - The conflicting privileges introduce risk when assigned to a user through multiple security objects.

Assessment Results

- Assessment Results
  - Understanding the results of the assessment in a relative and realistic context is critical to planning a successful remediation.
    - Most organizations identify hundreds or even thousands of individual Segregation of Duties conflicts during the assessment.
    - Most organizations will not be able to technically remediate all conflicts.
      - Volume of conflicts
      - Limited human resources in some geographies
      - Limited remediation resources or capabilities
      - Technological constraints
      - Business process constraints
  - Results should be prioritized in a way to address the high risk items as soon as possible. Key risk factors should be defined and contemplated.
    - Inherent risk of the conflict definition (qualitatively defined)
    - Risk of how frequent the conflict occurrence is (quantitatively defined)

Remediation Approach

- Technical Remediation
  - Security Redesign
    - Depending on the severity of the issues identified during the assessment, correcting existing security configuration may not be the most efficient path for remediation.
    - If a security redesign is necessary, this effort should be coordinated with other strategic security initiatives that may be underway (e.g. identity management, etc.). Often other initiatives can be leveraged in Segregation of Duties remediation.
  - Security Correction
    - Most organizations choose the path of correcting their existing security configuration for Segregation of Duties remediation.
- Process Remediation
  - It is highly unlikely that any organization can address all Segregation of Duties issues exclusively through technical remediation.
  - Process remediation involves introducing reporting, monitoring, or other mitigating controls that address technical weakness in regards to Segregation of Duties.
  - Consideration should also be given to pre-existing security administration processes in regards to Segregation of Duties.
    - Segregation of Duties standards must be maintained going forward
    - Contemplation of Segregation of Duties must be integrated into security administration processes

Remediation Approach

- Segregation of Duties Tools
  - Tools are beginning to emerge that address Segregation of Duties needs as a result of Sarbanes-Oxley compliance requirements.
  - The tool you select should address both the initial assessment and remediation project, and also the ongoing needs of the organization with respect to Segregation of Duties. To that end, a tool that can integrate with your organization's security provisioning/administration processes is most desirable.

approva

BizRights

For
SAP, Peoplesoft,
and Oracle

SECURINFO
Specialized Software Solutions

RISK MANAGER for SAP

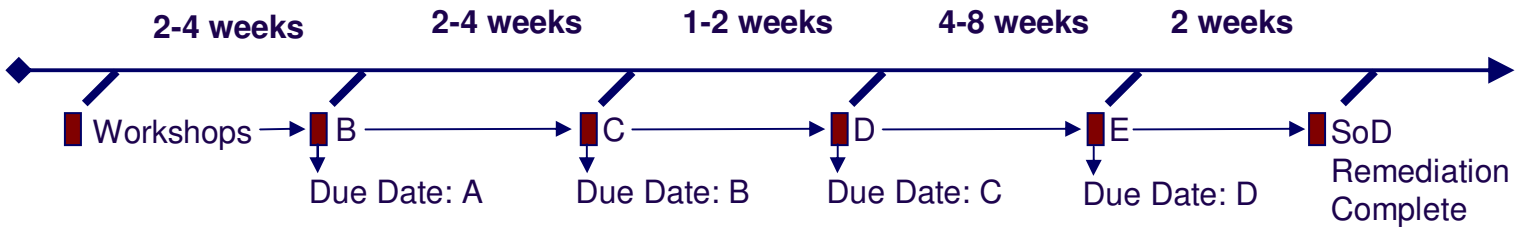
VIRSA™
Real-time Continuous Compliance

Compliance Calibrator

For
SAP

Project Lifecycle

- Overview of the Approach
  - A. Host internal workshops, education stakeholders and building consensus.
    1. Deliverable is a final, customized Segregation of Duties matrix that will serve as the rules for your organization
    2. Results are socialized for design feedback
  - B. Assessment reporting is generated to capture the SoD issues for remediation.
    1. Deliverables include detailed conflict definition reports and summary reporting and analysis
  - C. Functional business teams are provided with a copy of the final assessment reporting to gather feedback regarding the results and what remediation steps may be feasible. This facilitates a context for understanding the results.
    1. Deliverables include business area perspectives regarding feasible remediation steps and a remediation strategy
    2. Remediation strategy is socialized for design feedback
  - D. Security changes (technical and process remediation) are implemented pursuant to the decisions made by project teams. Controls are enhanced to reflect an ongoing contemplation of Segregation of Duties in the security management process.
    1. Deliverables include security configuration changes and update controls documentation
  - E. Segregation of Duties is reassessed to confirm the success of technical remediation changes.
    1. Deliverables include updated detailed conflict definition reports and summary reporting and analysis
    2. Final reporting is socialized to meet assurance needs



Deloitte.

QUESTIONS?????

Dan Hirstein
Director – ERS
(816) 802-7208
dhirstein@deloitte.com