INTERNAL AUDIT AND SARBANES OXLEY OVERVIEW

May 23, 2023

Presented by: Anthony DeLeon, Senior Manager
BDO - Risk Advisory Services

Section 1

Introduction

Agenda

1. **Introduction**
2. **Internal Audit Overview**
   - Internal Controls
   - COSO Management's Responsibility
   - Framework
   - Internal Control Business Process and IT Examples
3. **Sarbanes Oxley Overview**
   - What is SOX?
   - Phases of SOX
   - SOX General Concepts
   - Components of Walkthrough
   - Common Pitfalls
   - "Big Rules" of SOX
4. **Q&A**

How Will This Session Help You?

- Obtain a better understanding of **internal controls, corporate governance, fraud awareness** and **ethics**
- **Enhance** and strengthen **internal controls**
- **Enhance your contribution** to the organization
- **Protect employees** and morale
- Protect your **reputation**
- Enhance **profitability**

Section 2

Internal Audit Overview

Internal Controls - Definition

Internal control is broadly defined as a process, effected by an entity's board of directors, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

1. Reliability of financial reporting
2. Safeguarding of assets
3. Compliance with applicable laws and regulations
4. Effectiveness and efficiency of operations

Internal Controls – Management's Responsibility

What is management's responsibility concerning internal controls?

Management should design internal controls to ensure the reliability of financial reporting, safeguarding of assets, compliance with applicable laws and regulations and the effectiveness and efficiency of operations.

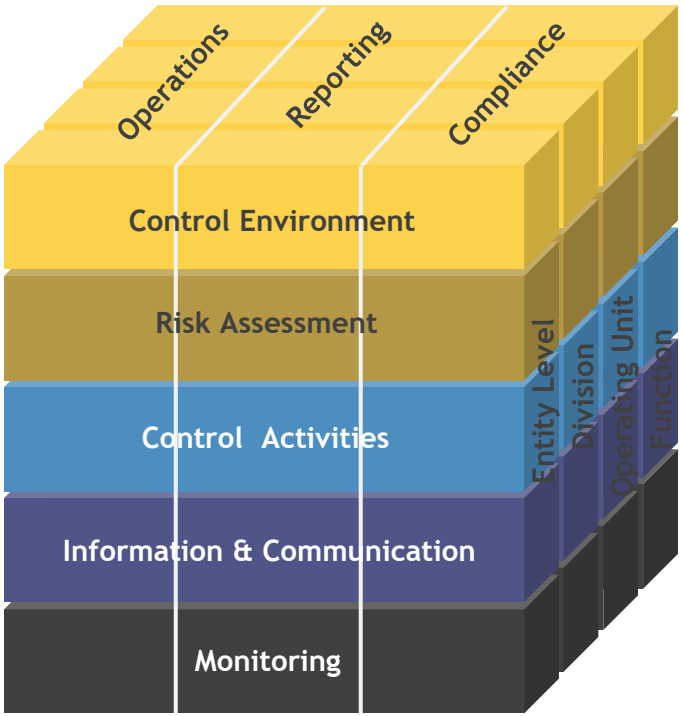
Internal Controls

- Entity level
- Business process
- Information technology

Internal Controls – COSO Framework

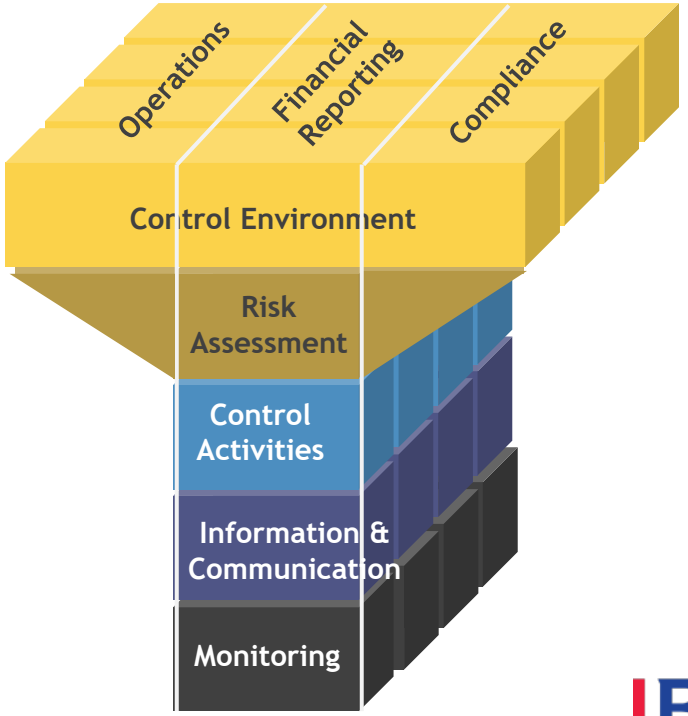
"Business Control"

2013 COSO Framework



"SOX" (Financial Reporting)

2013 COSO Compendium of Approaches



Internal Controls – Entity Level Controls Framework

COSO Principles			
#	Component Principle	Design Adequacy	Operating Effectiveness
I.	**Control Environment**	**Adequate**	**Effective**
	1. Demonstrates Commitment to Integrity and Ethical Values	Adequate	Effective
	2. Exercises Oversight Responsibility	Adequate	Effective
	3. Establishes Structure, Authority, and Responsibility	Adequate	Effective
	4. Demonstrates Commitment to Competence	Adequate	Effective
	5. Enforces Accountability	Adequate	Effective
II.	**Risk Assessment**	**Adequate**	**Effective**
	6. Specifies Suitable Objectives	Adequate	Effective
	7. Identifies and Analyzes Risks	Adequate	Effective
	8. Assesses Fraud Risk	Adequate	Effective
	9. Identifies and Analyzes Significant Change	Adequate	Effective
III.	**Control Activities**	**Adequate**	**Effective**
	10. Selects and Develops Control Activities	Adequate	Effective
	11. Selects and Develops General Controls over Technology	Adequate	Effective
	12. Deploys Through Policies and Procedures	Adequate	Effective
IV.	**Information & Communication**	**Adequate**	**Effective**
	13. Uses Relevant Information	Adequate	Effective
	14. Communicates Internally	Adequate	Effective
	15. Communicates Externally	Adequate	Effective
V.	**Monitoring**	**Adequate**	**Effective**
	16. Conducts Ongoing and/or Separate Evaluations	Adequate	Effective
	17. Evaluates and Communicates Deficiencies	Adequate	Effective

Internal Controls – Entity Level

Code of conduct and ethics	Organizational structure	Policies and procedures
Whistleblower hotline	Background checks and hiring procedures	Certification of internal controls
Physical segregation of duties	Logical segregation of duties within business applications	Review of monthly financial statements

Examples of Entity Level Controls

Code of conduct and ethics

Employee handbook

Compliance hotline

Conflicts of interest policy

Other company policies and procedures

Executive Committee

Board of Directors oversight

Enterprise risk management program

Internal Controls – Business Process

Procurement to Payables (Examples)

1. Bidding policy process
2. Approval of new vendors
3. Contract approval process
4. Review by independent person of changes made to vendor master file (e.g. Infinium, Puridiom)
5. Approval of capital authorization requests, purchase requisitions and invoices

Internal Controls – Business Process

Procurement to Payables (Examples)

6. Two or three way match - comparison of invoices to purchase orders and receipts
7. Approval of cash disbursements (checks, wire transfers and ACH)
8. Separate initiator and approver for wire transfers
9. Positive pay

Internal Controls – Business Process

Revenue to Receivables (Examples)

1. Approval of pricing and products or services
2. Approval of customer contracts
3. Review of proper pricing and products or services entered into application (e.g. Galaxy, ResortSuite, Infogenesis)
4. Approval of adjustments (e.g. refunds, overrings, pricing)
5. Reconciliation of cash receipts and revenue

Internal Controls – Business Process

Payroll (Examples)

1. Approval of changes to employee master file
2. Independent review of changes made to employee master file
3. Approval of timesheets
4. Review of payroll register
5. Authorization of payroll disbursements
6. Reconciliation of payroll to the general ledger

Internal Controls – Business Process

Inventory (Examples)

1. Receiving process
2. Physical safeguarding of assets
3. Requisitioning process and verification
4. Physical inventory count procedures and count oversight
5. Reconciliation of inventory to the general ledger

Internal Controls – Business Process

Financial Closing (Examples)

1. Financial closing calendar
2. Review and approval of journal entries
3. Review and approval of account reconciliations
4. Review and approval of financial statements and budget to actual analysis

Internal Controls – Information Technology

IT Entity Level Controls

- IT policies and procedures
- Organization

Application, Database & Operating System Change Management Controls

- Authorized, tested, and approved
- Segregation of duties

Network, Application, Database & Operating System Security Controls

- Authentication and authorization controls
- Validation and monitoring of appropriateness of access
- Segregation of duties

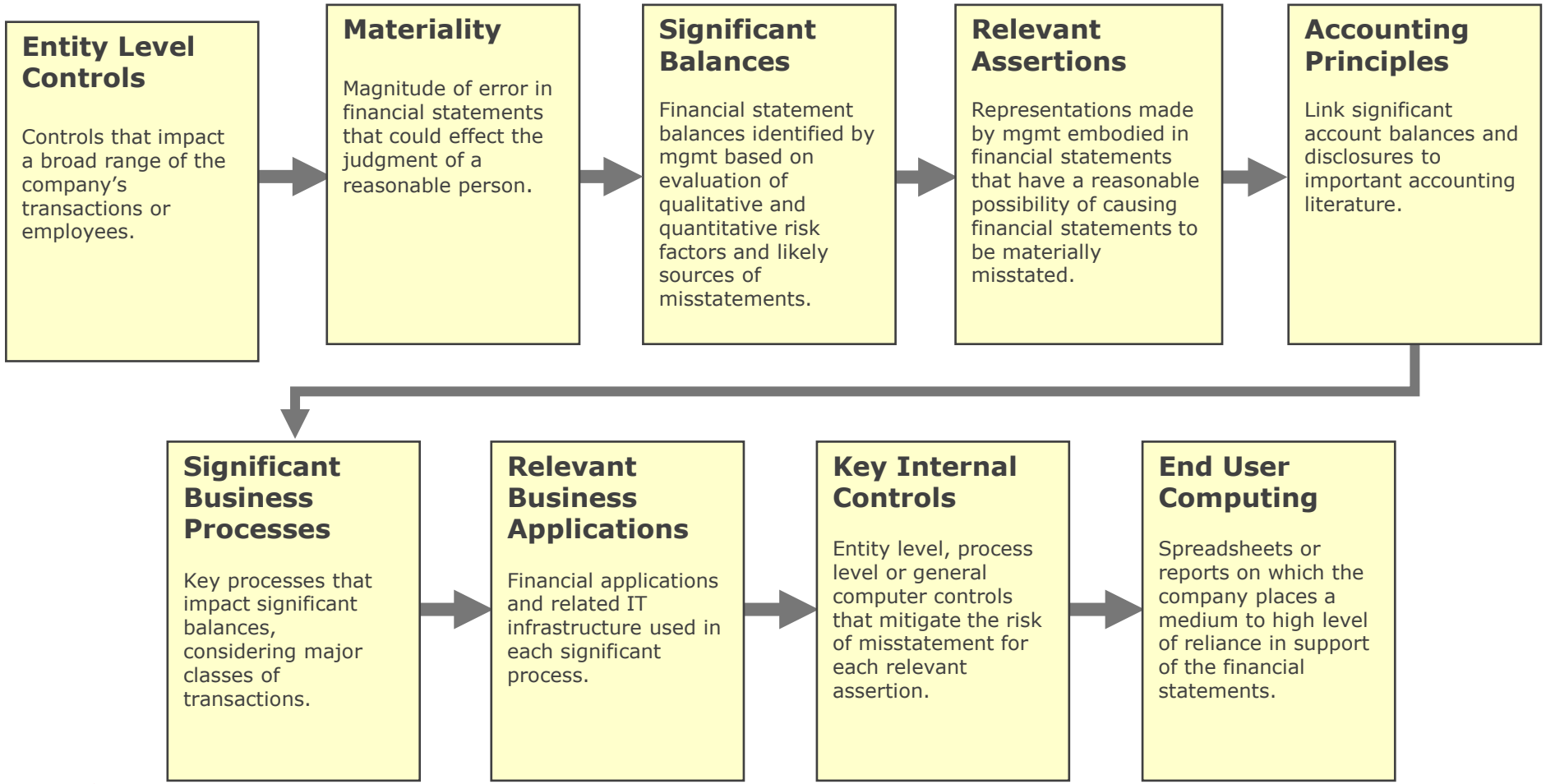
Data Backup and Recovery Controls

- Scope and effectiveness of backup and recovery procedures

Process Monitoring Controls

- Security
- Change management
- Problem management

Internal Controls – Financial Controls Top-Down Approach



Internal Controls – Manual vs. Automated

- **Manual Control**
  - Approval of purchase requisition in Procurement system

- **Automated Control**
  - Procurement system automatically preventing the same employee from being the preparer of the purchase requisition and approver of the purchase requisition

Internal Controls – Segregation of Duties

The basic idea underlying segregation of duties is that no employee or group of employees should be in a position both to **perpetrate** and **to conceal errors or fraud** in the normal course of their duties.

Internal Controls – Segregation of Duties

The principal incompatible duties to be segregated are:

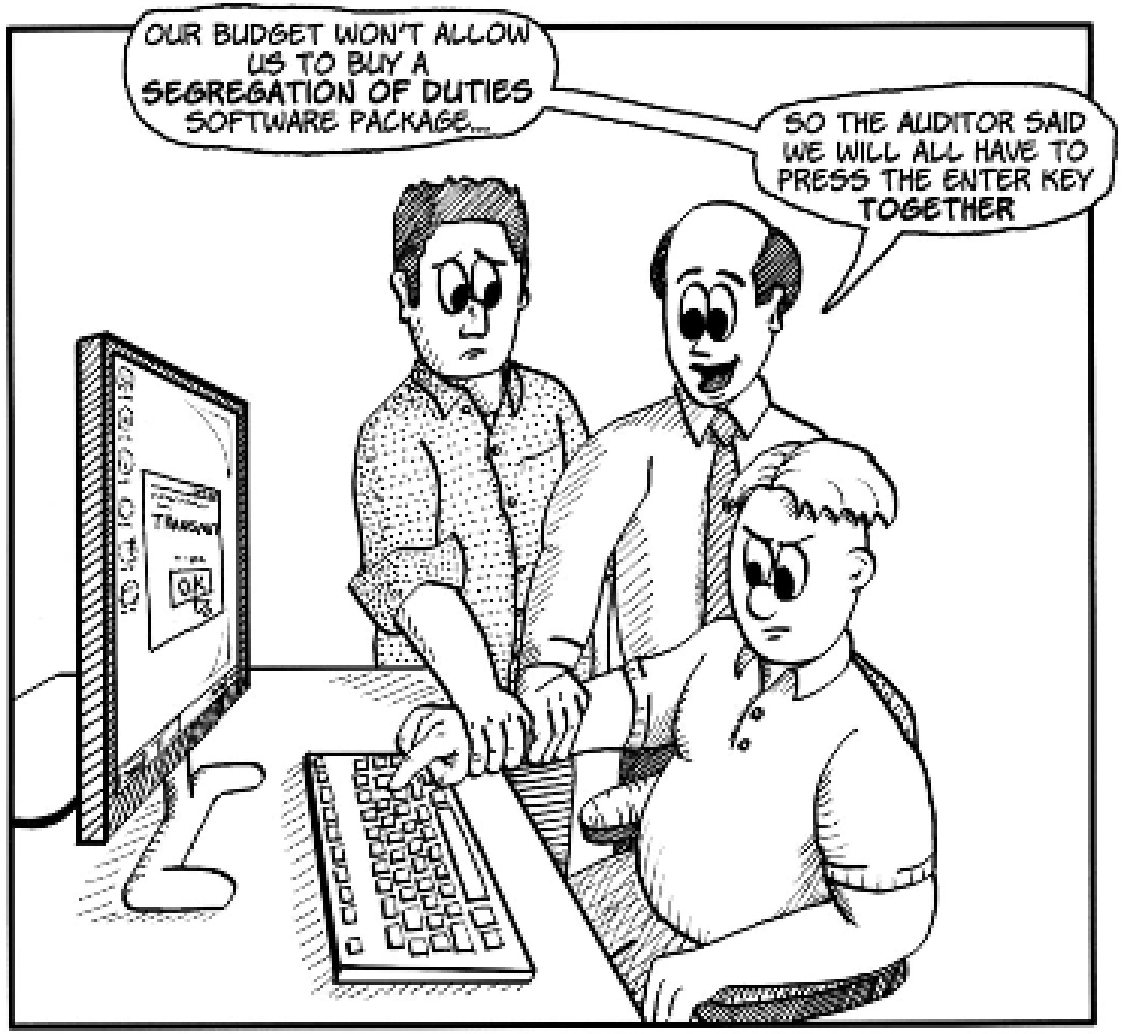
1. **Custody of assets** (e.g. execution of wire transfer, authorized signatory)
2. **Authorization** or approval of related transactions affecting those assets (e.g. approval of disbursements)
3. **Recording** or reporting of related transactions (e.g. recording of transaction in the general ledger)

Internal Controls – Segregation of Duties Example

Example – The Same Employee

- Approves vendor
- Approves and enters purchase order (PO)
- Receives inventory and enters into system
- Approves invoices
- Performs three way match of PO, receipt and invoice

Internal Controls – Segregation of Duties



Section 3

Sarbanes Oxley (SOX) Overview

Introduction

- The **Sarbanes-Oxley Act (SOX)** act was passed in 2002 to combat major accounting scandals from corporations like Enron and WorldCom. Its goal is to **reduce financial malfeasance** by increasing penalties for failing to meet accounting standards. It applies to all publicly traded US companies.

- **Penalties for financial statement fraud** or misstatement can include millions of dollars in **fines** and 20 years in **prison**.

- To ensure higher **standards of governance**, companies must establish and **comply** with internal controls on financial reporting (ICFR). These controls are **intended to protect** the integrity of the data that builds **financial records** and the integrity of the **annual report**.

- **CEO and CFO** provide **certification** over disclosure **controls** and effectiveness of controls.

What is SOX?

- Background
  - "SOX" refers the Sarbanes-Oxley Act, which was a bill enacted in the United States in 2002 in response to a number of corporate / accounting scandals
  - Requires the CEO and CFO of publicly-held companies to certify the accuracy of their financial results in public filings (Section 302)
  - Also requires annual assessments over the effectiveness of internal controls over financial reporting (Section 404)
  - Intent of the Sarbanes-Oxley Act is to protect investors by improving reliability and accuracy of corporate disclosures, which led to increased attention to accuracy and internal controls
- Benefits of compliance with SOX
  - Encourages a strong, cohesive internal control environment through enhancement of documentation, increased communication channels
  - Increased confidence in financial reporting
  - Can assist in the prevention or detection of fraud

Phases of SOX

- Risk Assessment
  - Risk Assessment is performed to determine the scope of SOX testing
  - Calculate a materiality figure, determine which locations have financial statement account balances that exceed that materiality
  - Identify and assess risk related to these financial statement accounts
  - Internal controls that address the identified risks will be identified or confirmed
- Planning and Scope
  - Finalize and confirm scope of testing
  - Schedule time at all in-scope locations for walkthrough conversations
- Process/Control Walkthrough Discussions
  - Discussion of processes and underlying internal controls with process owners. Controls are identified and the operation of the controls is verified
  - Controls are documented, or documentation is updated if needed

Phases of SOX (cont.)

- Test of Operating Effectiveness
  - Once we have determined controls are designed effectively, we perform testing to determine whether controls have been operating throughout the testing period
  - Testing is performed by selecting samples, requesting documentation and reviewing documentation
  - Testing exceptions (no documentation, control not performed) are known as “operating deficiencies”

SOX General Concepts: Controls

- A control is defined as any **action taken to mitigate or manage risk** and increase the probability that the business/process will achieve its goals and objectives. A control is in place to prevent an error from occurring or minimize the impact if it does occur. **Control activities are part of the process.**

Process

Finance
Relates to specific end to end financial processes and are incorporate in business activities

IT General Controls
Relate to specific systems/applications/ tools and are managed by IT

Control Method

Manual
Performed without IT technology interference
Example: Contract Manual Approval / Sign-Off

Mixed / IT Dependent Manual - ITDM
Performed by a person with the assistance of an IT technology
Example: Workflow Approvals in a System

Automated
Performed automatically by the IT technology without "human" interference
Example: 3-Way Match

Control Type

Preventive
Designed to prevent a risk from occurring by including review components or system restrictions on the front end

Detective / Corrective
Designed to detect/correct a potential material misstatement by incorporating reviews on the back end

Control / Not a Control

CONTROL	NOT A CONTROL
✓ Policy & Procedures	✓ Deliver report to supervisor
✓ Authorize	✓ Prepare document monthly
✓ Approve	✓ Generate month-end report
✓ Compare	✓ Deposit cash in bank
✓ Reconcile	✓ Submit report to SEC
✓ Analyze	
✓ Review	
✓ Validate	
✓ Separation of duties	

Components of a Walkthrough

- Performing walkthroughs is critical because it helps to confirm whether management:
  1) understands how a transaction goes through the process, including how IT is used to process or transfer data
  2) has identified all risks (or if we are missing some)
  3) has identified controls to address the risks (or potential gaps)
  4) understands the design of the controls well enough to know if they sufficiently address the risks (or if we need to clarify how the control is performed)
  5) has seen appropriate documentation to support the design of controls

Common Pitfalls

- Ineffective management of competing priorities
- Lack of consistent and timely performance of controls with contemporaneous documentation
- Inadequate segregation of duties
- Lack of appropriate precision and documentation of management review procedures
- Lack of documentation over the completeness and accuracy of critical reports and data used in spreadsheets
- Inappropriate user access to applications and lack of periodic review
- Privileged and administrative access rights to systems and applications not appropriately monitored
- Lack of controls around review and documented approval of new set-ups and changes to master file data
- Journal entries and supporting detail not reviewed and approved independent of preparer
- Account reconciliations and investigation of reconciling items not performed and reviewed on a timely basis
- Documented customer acceptance of quantity and price not received prior to shipment
- Lack of controls around cut-off
- Ineffective monitoring of interfaces and job scheduling
- Lack of testing and approval of system changes before movement from development to production

“Big Rules” of SOX

➢ Key Spreadsheets

- Key Spreadsheets are spreadsheets that directly impact or provide support in the initiation, authorization, recording, processing and reporting of financial transactions and disclosures
- Typically, these spreadsheets calculate an amount or amounts that are used in the control and/or recorded in financial statements
- When performing a review of key spreadsheets, the following should be considered:
  - Recalculation and confirmation of accuracy of key amounts in spreadsheet
  - Proper use of Excel functions/formulas in spreadsheets (functions use appropriate data, etc.)
  - Third party information brought into the spreadsheet is validated for completeness & accuracy
  - Ensure that key totals on the spreadsheet are the result of a formula and not hard-coded
  - Access to key spread sheets is limited

“Big Rules” of SOX

- Performance of Review
  - When a review of a transaction, report, reconciliation or anything else is performed as part of a control, evidence should be provided to demonstrate its performance
  - Reviews should include verification of completeness and accuracy of information used in the control, the accuracy of the activity in the control and that the appropriate procedures have been followed

- Documenting Approval
  - Documentation of control approval can be provided using the following methods:
    - Signature on physical documents – signature should include printed name, title and date at signature line
    - Email to preparer or other parties noting that review was performed, and approval provided
    - Electronic indication of approval through workflow within a system

“Big Rules” of SOX

➢ Management Review Controls

- Management Review Controls include reviews of calculations, valuations, development of assumptions, reconciliations, analyses prepared by others (including third parties), or reviews of financial results against budgets and/or prior periods.
- MRCs can vary in their nature from controls with a simple review element to complex controls with significant judgment, management assumptions, and numerous control activities (we refer to these controls as multi-layered MRCs).
- Fundamental Elements of Management Review Controls:
  - Nature of Review Procedures – Specific steps taken by review owner
  - Level of Precision – Criteria used by control owner to drive investigation and review procedures
  - Evidence of Review Performed – Must go beyond sign-off and provide description of the performance of each review activity prescribed in control

“Big Rules” of SOX

- Variance Threshold
  - While preparing balance sheet account reconciliations, differences between the subledger and general ledger above 0.5% or $5,000 should be investigated, explained and resolved
- Maintaining, Keeping and Storing Documentation
  - Documentation saved related to the performance of internal controls
  - Maintain a “SOX” folder on your hard drive or the network drive
  - Archive emails
- Timeliness
  - Documentation should be prepared and retained at time of control performance
- Communicating Changes
  - Changes in the design of a control (performer, system, method) should be communicated to the Project Manager so the control can be updated on the control matrix

Section 4

Questions?

BDO is the brand name for BDO USA, LLP, a U.S. professional services firm providing assurance, tax, and advisory services to a wide range of publicly traded and privately held companies. For more than 100 years, BDO has provided quality service through the active involvement of experienced and committed professionals. The firm serves clients through more than 65 offices and over 700 independent alliance firm locations nationwide.

As an independent Member Firm of BDO International Limited, BDO serves multi-national clients through a global network of more than 88,000 people working out of more than 1,600 offices across 167 countries and territories.

BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms.

www.bdo.com