McKONLY & ASBURY

SOX: Are You Still Testing Too Many Controls?

macpas.com

Introductions

Elaine Nissley, CISA, PMP, CRMA, CRISC, CCSFP, CCP, CCA

Director

- Over 30 Years of Internal Audit and Internal Controls Experience
- Leads the Internal Audit and CMMC Practices
- Provides Internal Audit Outsourcing services
- Sarbanes Oxley and OMB Circular A-123 Compliance
- NIST 800-53 based Independent Assessments

Victor Kong, CIA, CRMA, CCSA, qAC, CFE

Senior Manager

- Over 18 years of Internal Audit and Internal Controls Experience
- Leads Internal Audit or Sarbanes-Oxley projects
- Experienced EQA Assessor

Firm Overview

Helping You Thrive!

McKonly & Asbury

M&A is a team of CPAs and Business Advisors serving clients from our offices in Camp Hill, Lancaster, Bloomsburg, and Philadelphia.

accountingTODAY 2024 Best Firms to Work For

accountingTODAY 2024 Best Firms for Young Accountants

accountingTODAY 2024 Best Firms for Women

BEST PLACES to work in PA 2024

Services Provided

- Advisory & Business Consulting
- Audit & Assurance
- Tax
- Entrepreneurial Support & Outsourced Accounting
- SOC & Technology Consulting

Industries Served

- Affordable Housing
- Architecture, Engineering, and Construction (AEC)
- Entrepreneurial
- Family-owned Business
- Franchises
- Healthcare
- Manufacturing & Distribution
- Nonprofit
- Public Companies

Objectives

- Explore the number of controls needed to comply with SOX internal control requirements.
- Understand control rationalization.
- Understand what areas of ITGC must be include in the testing of ICFR.

McKONLY & ASBURY

How Many ICFR Controls?

Risk Based Approach

Objectives

- SOX and ICFR
- Average Number of Controls
- Types and Categories of Controls
- Effectiveness of Controls
- Control Challenges
- Risk Based Approach & Best Practices

Purpose of SOX

- Established in 2002 in response to corporate scandals (Enron, WorldCom) to protect investors and ensure accurate financial reporting.
- Section 404 requires management to assess and report on the effectiveness of internal controls over financial reporting (ICFR).
- SOX Section 404
  - ✓ Requires companies to establish, maintain, and evaluate the effectiveness of internal controls over financial reporting.
  - ✓ External auditors must assess and report on management's evaluation.

Importance of ICFR

- **Reasonable Assurance**
  - ✓ **Integrity of financial reporting, safeguarding assets, and compliance with regulations**
- **Effective ICFR Helps to Protect Financial Statement from**
  - ✓ **Errors, Fraud, and Misstatements**
- **Objectives of ICFR**
  - ✓ **Accuracy and completeness of financial reporting**
  - ✓ **Timely preparation and submission of reports**
  - ✓ **Preventive and detective controls to identify and mitigate risks**

Average Number of ICFR

- **Controls Frameworks**
  - ✓ **US standard is COSO (Committee of Sponsoring Organizations of the Treadway Commission)**
- **Average Number of Controls**
  - ✓ **The greater the complexity and de-centralization the greater the number of controls**
  - ✓ **Maturity of the Governance Environment impacts the number of controls**
  - ✓ **Public companies typically range from 100 – 300 controls for SOX 404**

Categories of Controls

- **Entity-Level Controls**
  - ✓ Organization controls that impact the entire financial reporting process
  - ✓ Corporate governance, risk management policies, human resources
  - ✓ Tone at the top, board oversight, business code of conduct, hiring and evaluation processes, training
- **Process-Level Controls**
  - ✓ Specific controls implemented within a financial process.
  - ✓ Payroll processing, accounts payable and receivable controls, and journal entry approvals

Categories of Controls

- **IT General Controls**
  - ✓ Controls over IT systems that support financial reporting
  - ✓ Access controls, data backups, and system development lifecycle/change management controls
- **Third-Party Vendor Controls**
  - ✓ Controls over IT systems that support financial reporting
  - ✓ Access controls
  - ✓ SOC 1 or SOC 2 Type 2 Report

Effectiveness of Controls

- **Assessment of Effectiveness**
  - ✓ Assess effectiveness and strengthen weak controls
  - ✓ Assessment of effectiveness by internal control experts
  - ✓ External Auditors assess the internal evaluation of the controls
- **Key Considerations**
  - ✓ Document and evidence controls
  - ✓ Regular monitoring and testing
  - ✓ Test early and leave time for remediation

Control Implementation Challenges

- **Common Issues**
  - ✓ Weak Segregation of Duties
  - ✓ Lack of documentation
  - ✓ Outdated IT systems or weak system of ITGC
  - ✓ Failure to remediate control issues timely
- **Impact of Control Weaknesses**
  - ✓ Restatement of Financial Statements
  - ✓ Loss of investor confidence
  - ✓ Regulatory penalties, fines, and jail time

Risk Based Approach

- Assess the Control Environment (Governance Controls)
  - ✓ Strong control environments
    - Reduces the need to test detailed controls
    - Can obtain reasonable assurance by testing review and governance controls
- Weak Control Environment
  - ✓ Reduces management's reliance on daily and weekly controls, thus increasing the number of controls included in the testing population.

Best Practices

- Comprehensive Documentation
- Regular Training
- Continuous Improvement
- Automation of Controls
- Independent Assessments

McKONLY & ASBURY

SOX Control Rationalization

Understanding SOX Control Rationalization

- Streamlining Compliance to Enhance Efficiency and Reduce Risk

Agenda – SOX Control Rationalization

- What is SOX Control Rationalization?
- Objectives of Control Rationalization
- Key Benefits
- Challenges
- Steps in the Rationalization Process
- Tools & Techniques
- Takeaways

What is SOX Control Rationalization?

- A process to evaluate, streamline, & optimize SOX-related controls.
- Focuses on eliminating redundant, low-value controls and prioritizing high-impact ones.
- Ensure controls address key risks without unnecessary complexity.

Why Rationalize Controls?

- Overlapping controls often lead to inefficiency.
- Testing redundant controls wastes time and resources.
- Excessive controls dilute focus from critical risk areas.

Objectives of SOX Control Rationalization

- Reduce redundancy
- Focus on high-risk, high-value controls
- Improve cost efficiency
- Simplify audit processes
- Enhance control effectiveness

Benefits of SOX Control Rationalization

- Cost reduction in testing and auditing
- Streamlined control environment
- Improved focus on critical controls
- Enhanced compliance and governance

Common Challenges

- Resistance to change from process owners
- Alignment with stakeholders (e.g., auditors)
- Risk of removing critical controls
- Ensuring documentation satisfies auditors and regulators

Steps in SOX Control Rationalization

- High level outline of the process:
  - ✓ Inventory Existing Controls
  - ✓ Risk Assessment
  - ✓ Evaluate Control Effectiveness
  - ✓ Prioritize Key Controls
  - ✓ Standardize and Automate
  - ✓ Consult Stakeholders
  - ✓ Document Changes

Step 1: Inventory Existing Controls

- ✓ Catalog all SOX controls
- ✓ Identify
  - ✓ Redundancies
  - ✓ Overlaps.

Step 2: Risk Assessment

- ✓ Map controls to financial reporting risks
- ✓ Prioritize high-impact areas.

Step 3: Evaluate Control Effectiveness

- ✓ Assess control effectiveness
- ✓ Remove/merge redundant controls

Step 4: Prioritize Key Controls

- ✓ Map controls to financial reporting risks
- ✓ Prioritize high-impact areas.

Step 5: Standardize and Automate

- ✓ Use technology to automate
- ✓ Standardize repetitive processes.

Step 6: Consult Stakeholders

Engage to Align Changes

- ✓ Auditors
- ✓ Compliance teams
- ✓ Management

Step 7: Document Changes

Ensure all changes are documented for:

- ✓ **Auditors**
- ✓ **Regulators**

Tools & Techniques for Rationalization

- Risk & Control Matrices (RCM)
- Process Mapping Software
- GRC Platforms (e.g., AuditBoard, Workiva)
- Risk-based Testing and Data Analytics

Key Takeaways

- **SOX control rationalization**
  - ✓ **Improves efficiency**
  - ✓ **Reduces costs**
  - ✓ **Strengthens compliance.**
- **A systematic, risk-based approach is critical.**
- **Collaboration with stakeholders ensures success.**

McKONLY & ASBURY

ITGC & ICFR

How much is too much?

Objectives

- Understand why ITGC is important for ICFR
- ITGC Risk Assessment and Scoping
- Core ITGC
- Future Trends in ITGC

Importance of ITGC

- **Information Technology General Controls Provide Assurance**
  - Accuracy/Reliability
  - Completeness
  - Security/Confidentiality
  - Failure to remediate control issues timely
- **Adverse ICFR Assessment by Auditors ***
  - 54.5% – Information technology
  - 53.7% – Accounting Personnel Resources
  - 39.7% – Inadequate Disclosure Controls
  - 39.3% – Segregation of Duties
  - 14.4% – Nonroutine Transactions

*Ideagen Audit Analytics North America, SOX 404 Disclosures: A 19-Year Review 2004 – 2022, 2022.

Importance of ITGC

- **Weak Access Controls**
  - ✓ Lack of Segregation of Duties & Excessive User Privileges
  - ✓ Weak Passwords & User Monitoring
  - ✓ Delayed Removal of Access (Transferred/Separated Employees & Contractors)
- **Inadequate Change Management**
  - ✓ Lack of Segregation (Development & Production Access)
  - ✓ Change from Waterfall to Agile (Developer Autonomy)
  - ✓ Lack of Business User Involvement

Importance of ITGC

- **Inadequate IT Governance and Oversight**
  - ✓ Insufficient Management Oversight of IT Controls
  - ✓ Lack of Operations Involvement
- **Lack of Training and Awareness**
  - ✓ Employees Lack of Training &Awareness of IT Controls
  - ✓ Abdication of Operations Responsibility to IT
  - ✓ Lack of Communication Between IT and Operations

Importance of ITGC

- **Incomplete Identification of Significant Financial Systems**

  - ✓ **Ongoing Risk Assessment of Information Systems**

  - ✓ **Third Party Systems SOC 1 and/or SOC 2**

Risk Assessment and Scoping

- Risk Based Assessment and Scoping
- Focus on Critical Financial Reporting Systems and Data
- Core ITGC Areas for Scoping

Risk Assessment/Scoping Key Steps

- Financial Reporting Systems IT Dependencies
- Evaluate ITGC Areas of Risk
- Assess IT Risk
- Regular Review
- Challenges

Critical Financial Systems

- Material Systems
- Critical Applications
- Internal and External IT Dependencies

Core ITGC

Access Controls

- User Access Management
- Segregation of Duties
  - ✓ Applications
  - ✓ Infrastructure
- Authentication Controls
  - ✓ Strong Passwords
  - ✓ Multi-factor Authentication

Core ITGC

Change Management

- **Change Control (Applications and Infrastructure)**
  - ✓ Authorized
  - ✓ Tested
  - ✓ Documented
- **Audit Trails**
  - ✓ Record System Changes
  - ✓ Monitor Compliance with ICFR

Core ITGC

- Data backup and Recovery
  - ✓ Availability
  - ✓ Integrity
- System Monitoring and Logging
  - ✓ Detect Irregular Acuities, Security Breaches & System Malfunctions
  - ✓ May Impact Financial Data
- Monitoring and Incident Management
  - ✓ Functioning properly
  - ✓ Detect Errors & Malicious Activities
  - ✓ Quick Response to Incidents

Future Trends in ITGC

- Automation of ITGC Monitoring
- Cybersecurity
- Cloud Computing
- Continuous Monitoring

ITGC in Summary

“Information technology and business are becoming inextricably interwoven. I don't think anybody can talk meaningfully about one without talking about the other.”

Bill Gates, “Business @ the Speed of Thought” 1999

McKONLY & ASBURY

Questions?

Contact Information

Elaine Nissley, CISA, PMP, CRMA, CRISC, CCSFP, CCP, CCA
Director

enissley@mapcas.com

717-972-5728

Victor Kong, CIA, CRMA, CCSA, qAC, CFE
Senior Manager

vkong@macpas.com

717-298-7494

McKONLY & ASBURY

Upcoming Events

March 27 Webinar

Tax Cuts and Jobs Act – Valuation/Tax Implications of a Sunset vs an Extension

REGISTER NOW