Internal Controls: Facts and Fiction

Colin Wallace, Partner – Advisory Services
The material appearing in this presentation is for informational purposes only and should not be construed as advice of any kind, including, without limitation, legal, accounting, or investment advice. 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 this information may have been prepared by professionals, it should not be used as a substitute for professional services. If legal, accounting, investment, or other professional advice is required, the services of a professional should be sought.

Assurance, tax, and consulting offered through Moss Adams LLP. Wealth management offered through Moss Adams Wealth Advisors LLC. Investment banking offered through Moss Adams Capital LLC.
Colin Wallace, CPA, CFF, CFE, CISA, CIA, CGAP
Partner

Colin has provided management consulting and internal audit services to public, private, government, and not-for-profit organizations since 2002. He has organized and performed financial, operational, and compliance audits throughout the United States and abroad, and has worked on all aspects of the internal audit process including planning, analysis, reporting, and project management.

Colin has led numerous fraud investigations involving misappropriation and misuse of company assets, the Foreign Corrupt Practices Act, and management override of internal controls. In addition, he has managed significant SOX 404 assessment projects and SOC examination engagements from initial implementation to final reporting.
Learning Outcomes

- Identify the updated areas of internal control failures and the number one factor contributing to a strong control environment.

- Draw the correlation between high profile news headlines and current trends with the need to examine risk and controls.

- Take away an actionable list of audit plan hot spots (with recommended actions) back to the workplace.
Agenda

• Why Examine Risk and Controls?
• Assessing the State of Your Controls
• Controls Maturity Across the Three COSO Objectives
• Building and Strengthening Your Internal Controls Environment
• Information Technology Controls
• Segregation of Duties
• Third-Party Service Provider Controls
• Hot Topic Areas
• Key Takeaways
Why Examine Risk and Controls?
Why Examine Risk and Controls?

- **FACT.** Good controls reduce the exposures inherent with the current economic environment.

- **FACT.** Good controls allow scalable and controlled organization growth, not just fraud prevention.

- **FACT.** Good controls increase the operational effectiveness of your organization by detecting errors and reducing rework.

- **FICTION.** Good controls remain the same and do not need review.

- **FICTION.** A risk assessment is sufficient for establishing strong internal controls.
Why Examine Risk and Controls?

• If your company hasn’t examined their internal controls in the past two years, it’s time to update them.

• If your company passes certain milestones, it’s time to update your internal controls policies and procedures.

• Areas that impact internal controls:
  - Updated guidance
  - Mergers/acquisitions
  - Fraudulent activity/suspected fraud
  - New/update of an ERP system
  - Growth
  - Revenue
  - Plans to take on investors
  - Plans for a public offering
Potential Exposures

- Fraud risks
  - Fraudulent financial reporting
  - Misappropriation of assets
  - Expenditures and liabilities for improper purposes
  - Fraudulently obtained revenue and assets, and costs and expenses avoided

- Inaccurate financial and managerial reporting
  - Inability to make sound financial and operational decisions

- Lost efficiencies
  - Duplication of effort
  - Failure to execute on strategic and operational objectives

- Compliance and reputation risk
  - News headlines
Areas Impacted by Controls

- Financial reporting
- Effective operations/resource management
- Compliance with laws and regulations
- Strategy and operational alignment
- Safeguarding of assets/fraud prevention
Current Trends

- Common themes in recent events:
  - Internal controls are good; management and auditors cannot ignore internal controls any longer
  - Internal controls are essential for all organizations
    - Start-up, developing, and mature organizations
    - Private or public organizations
    - Large and small entities
  - New developments in internal control
    - “How to Assess” vs. “Good Control Design”
    - “Top-Down” vs. “Bottom-Up” approach
  - More stringent guidelines enacted by COSO and the PCAOB
Internal Control Failures in the News

- Breached Hong Kong’s Code of Conduct
- Conflict of interest between discretionary order dealers and principal account dealers
- Failure of proper disclosure of its short-selling order
- Failure of the maintenance of unsystematic documentation of its electronic trading systems

Morgan Stanley Fined $2.4M on Internal Control Failures

Misstated SEC filings from 2011-2013
- Overstated subsidiary revenues and profits
- History of unaddressed material weaknesses in their filings
- Stock was delisted
- The SEC Enforcement Division retains the right to reopen the case

Advanced Emissions Solutions, Inc. fined $500,000 civil penalty
Assessing the State of Your Controls
Actions To Be Taken

Risk Scoping and Planning
- Document Reviews
- Management Interviews
- Observation

Risk Identification
- Entity Level
- Financial Reporting
- Operational
- Fraud
- Information Technology
- Compliance

Risk Assessment
- Likelihood
- Magnitude
- Total Risk

Manage Risk Response
- Avoid
- Accept
- Share
- Reduce

Internal Audit Work Plan
- Conduct Audits
- Report Audits
- Track Corrective Action

Internal Audit Work Plan

Risk Assessment

.manage risk response

- avoid
- accept
- share
- reduce

Internal Audit Work Plan
Defining Your Risk Universe

Enterprise risk assessments:

- Broadly survey the organization
- Identify risks to accomplishing organizational objectives
- Present a balanced snapshot of risks
- Allow for focus of internal audit efforts
Risk Assessment Factors

- **Risk Factors – Impact**
  - Effect on goals achievement
  - Financial amounts at risk
  - Regulatory compliance and system compliance
  - Health and/or safety
  - Billing and revenue capture exposures
  - Cost or operational concerns
  - Contractual compliance

- **Risk Factors – Likelihood**
  - Probability of potential problem, loss, or missed opportunity
  - Potential timeframe for undesirable outcome
  - Management concerns
  - Operations structure, changes, and complexity
  - Regulatory changes
  - Financial incentives
  - Past issues
  - Asset liquidity
Linking Risk to Processes and Controls

[Diagram showing the linking of risk to processes and controls, with axes for likelihood of control/process issues and importance to business performance.]
Rating and Responding to Risks

Consider Cost/Benefit of Controls

- What should you focus on?
- Leverage automated controls
- Determine desired level of control assurance relative to risk

Effects of Compensating Controls

- What can you do to improve?
  - When identifying controls, look for IT controls first
  - Before implementing a new control activity ask, “What could go wrong?” Is there another control that limits maximum exposure?
  - Always compare likelihood and magnitude of exposure to proposed control and evaluate cost/benefit
Rating and Responding to Risks

Tie Risks to Strategic Plans

- Reflect strategic priorities in budgeting decisions
- Budgets must reflect the top-down commitment to address current risk and emerging risk

“If you fail to plan, you are planning to fail.” – BENJAMIN FRANKLIN
Controls Maturity Across the Three COSO Objectives
Controls Maturity Across the Three COSO Objectives

- **Operations**: Effective and efficient use of resources
- **Reporting**: Preparation of internal and external financial and non-financial reporting
- **Compliance**: Compliance with laws and regulations
Control Environment Maturity

**Level 1 Unreliable**
Unpredictable environment where control activities are not designed or in place.

**Level 2 Informal**
Disclosure activities and controls are designed and in place.
Controls are not adequately documented; controls mostly dependent on people.
No formal training or communication of control activities.

**Level 3 Standardized**
Control activities are designed and in place.
Control activities have been documented and communicated to employees.
Deviations from control activities will likely not be detected.

**Level 4 Monitored**
Standardized controls with periodic testing for effective design and operation with reporting to management.
Automation and tools may be used in a limited way to support control activities.

**Level 5 Optimized**
An integrated internal control framework with real-time monitoring by management with continuous improvement (enterprise-wide risk management).
## Improved Controls Reliability

<table>
<thead>
<tr>
<th>Less Assurance</th>
<th>Greater Reliability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indirect coverage of risk</td>
<td>Direct coverage of risk</td>
</tr>
<tr>
<td>Manual control</td>
<td>Automated control</td>
</tr>
<tr>
<td>Complex control</td>
<td>Simple control</td>
</tr>
<tr>
<td>Detective control</td>
<td>Preventive control</td>
</tr>
<tr>
<td>Inexperienced personnel</td>
<td>Experienced personnel</td>
</tr>
<tr>
<td>Single control</td>
<td>Multiple, complementary, or redundant controls</td>
</tr>
<tr>
<td>High level analytic</td>
<td>Detailed transaction coverage</td>
</tr>
<tr>
<td>Weak segregation of duties</td>
<td>Strong segregation of duties</td>
</tr>
<tr>
<td>Partial audit period coverage</td>
<td>Full audit period coverage</td>
</tr>
<tr>
<td>Control occurs well after transaction processing</td>
<td>Control occurs in real time</td>
</tr>
</tbody>
</table>
Building and Strengthening Your Internal Controls Environment
Building and Strengthening Your Internal Controls Environment

- Senior leadership buy-in is critical in implementing and monitoring controls; you are setting the tone at the top
- Policies and procedures documenting controls should be complete, user friendly and regularly reviewed
- All personnel should be required to acknowledge and adhere to policies and procedures
- Controls that are not implemented do not help achieve desired results

Senior Management commitment to strong internal controls is the number one factor to a strong control environment.
Key Challenges

- Factors for aligning internal audit with corporate strategy
  - Differing/competing expectations from stakeholders (e.g., government, citizens, regulators, governing bodies, leadership, other departments)
  - Buy-in from multiple department heads and obtaining broad participation throughout the organization
  - Use of definitions for risk and value
  - Competency, trust and credibility of the role of internal audit
  - Alignment of risks to business objectives and strategic plans
  - The speed of change
  - Divided team focus may not contribute to critical thinking i.e., a junior auditor focusing on SOX
Building and Strengthening Your Internal Controls Environment

Key Principles:

• Align internal audit with corporate strategy

• Integrity and ethical values
  - Board of directors
  - Management philosophy and operating style
  - Organizational structure

• Commitment to competence
  - Authority and responsibility
  - Human resources
Level of Precision

Important, but Indirect
- Board of Directors meeting

Direct, but Not Precise
- Department head review of flash reports

Direct and Precise
- Month-end close accounting review meeting
- Budget to actual comparisons
- Headcount and salary fluctuation review
- Covenant calculations of capital outlays
- Obsolete and overstock inventory
Information Technology Controls
IT General Controls Impact Control Reliability

As with any system, technology has its share of risk and uncertainty which may lead to questions such as:

- Is my data available and reliable?
- Who has access to my systems?
- What is the source of my data?
- Who can change my data or the functionality of my applications?
- Has my system been implemented properly?
IT General Control Domains and Examples

- **Security**
  User provisioning controls, restricted privileged access, periodic user access review, physical security

- **Change Management**
  Segregation of duties, restricted access to application source code, user acceptance testing

- **System Development**
  Data conversion testing, “go-live” approval, functional testing by end users

- **Computer Operations**
  Backup and restoration of critical data, monitoring of processing results
Common Types of Application Controls

- **Input and Access Controls**
  Data checks and validations; automated authorization, approval, and override; segregation of duties

- **File and Data Transmission Controls**
  Error logs, exception reporting, etc.

- **Processing Controls**
  Automated file identification and validation, functionality and calculations, audit trails and overrides, interface balancing, duplicate checks

- **Output Controls**
  General ledger and sub-ledger posting, update authorization, reporting
Application Control Objectives

- Input data is accurate, complete, authorized, and correct
- Data is processed as intended in an acceptable time period
- Output and stored data is accurate and complete
- A record is maintained to track data processing from input to storage to output
Application Control Benefits

- **Reliability**
  Reduces likelihood of errors due to manual intervention

- **Benchmarking**
  Reliance on IT general controls can lead to concluding the application controls are effective year to year without retesting

- **Time and Cost Savings**
  Typically, application controls take less time to test and only require testing once as long as the IT general controls are effective
Segregation of Duties Controls
Segregation of Duties Controls—Facts

• Segregation (separation) of duties (SOD) is a critical element of internal controls
• SOD means more than one person is required to complete a function or task
• SOD controls and processes are designed to implement a system of checks and balances
• SOD is vital in preventing fraud and helps reduce or prevent errors
• SOD is necessary for organizations of all sizes
  - Challenging for organizations with limited staff or remote locations
  - Think outside of the box to implement adequate controls
  - May involve additional training
Segregation of Duties Controls—Facts

- SOD conflicts are not equally important to every organization. Examples include:
  - Safeguarding of assets versus financial reporting risks
  - Relative importance of information confidentiality
  - Nature of organization assets
  - Reduced risk when the “chain” of access is broken
Segregation of Duties Controls—Fiction

Common misconceptions about segregation of duties include:

• Fiction: SOD controls are IT controls
  - System-enforced access controls that are part of SOD controls generally rely on IT systems to operate and are often erroneously considered IT controls. SOD is a business control.

• Fiction: SOD controls are the same priority as other transaction-level internal controls
  - Assigning a lower level of security prioritization to SOD usually results in poorly designed system access rights and other inefficient or ineffective SOD security processes.
The Fraud Triangle

Opportunity
Pressure/Incentive
Rationalization
Third-Party Service Provider Controls
Third-Party Service Provider Controls Overview

- Understanding controls in place at third-party service providers is necessary to ensure a full assessment of an organization’s internal controls.
- Third-party service providers may:
  - Perform complex calculations on behalf of the company
  - Ensure your employees are paid timely and appropriately
  - Have physical custody of your systems and data
  - Collect data on your behalf

The real question is: Why wouldn’t you want to understand how your company’s operations and finances are impacted?
What You Can Do

How can you protect your company?

• Review internal controls of existing vendors:
  - Understand how your vendor’s operations impact your company
  - Obtain and review the SOC report from your providers
  - Perform your own inquiry and test vendor procedures around highest risk areas to your company (e.g., review list of vendor employees that can access your servers in a data center, review specifications and sign-offs of processes and procedures, etc.).

• Review internal controls of prospective vendors

• Manage identified risk through the introduction of internal controls
Hot Topic Areas
## Hot Topic Areas

<table>
<thead>
<tr>
<th>Audit Plan Hot Spot</th>
<th>Basic Controls Discipline</th>
<th>Risks</th>
<th>Recommended Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Contingency Planning</td>
<td>• Macroeconomic crisis preparedness</td>
<td>• Reputational damage</td>
<td>• Risk management system reviews</td>
</tr>
<tr>
<td></td>
<td>• Catastrophic systems failures</td>
<td>• Third-party/supply chain exposure</td>
<td>• Evaluate supply chain management</td>
</tr>
<tr>
<td></td>
<td>• Massive data breaches</td>
<td>• Disruptive cyber attacks</td>
<td>• Incident response and escalation audit</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Scenario planning workshop</td>
</tr>
<tr>
<td>2. Strategy Creation and Execution</td>
<td>• Uncertain growth assumptions</td>
<td>• Misplaced strategic initiatives</td>
<td>• IT capacity management audit</td>
</tr>
<tr>
<td></td>
<td>• Senior management decision paralysis</td>
<td>• Reduced growth</td>
<td>• Crisis management response audit</td>
</tr>
<tr>
<td></td>
<td>• The Strategy-Execution Gap (Hoshin Kanri)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Strategic planning process audit</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Strategy cascade audit</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Performance management audit</td>
</tr>
</tbody>
</table>
Hot Topic Areas

<table>
<thead>
<tr>
<th>Audit Plan Hot Spot</th>
<th>Basic Controls Discipline</th>
<th>Risks</th>
<th>Recommended Actions</th>
</tr>
</thead>
</table>
| 3: Corruption and Bribery | • Dependence on local intermediaries  
• Management overrides of internal controls  
• Mismatch of risks and control resources | • Third-party risk  
• Local tone at the top breakdown  
• Employee underreporting  
• Country risk | • Trend analysis of enforcement agency findings  
• Management Anti-Corruption Awareness Review  
• Intermediary due diligence audit  
• Anti-corruption risk assessment |
| 4: Tax Management     | • Information complexity and overload  
• More regulatory focus on transfer pricing  
• Unpredictable tax jurisdictions | • Increased likelihood of material weaknesses  
• Lost tax planning opportunities  
• Reputational damage | • Tax risk management assessment  
• Tax-sensitized data quality evaluation  
• Tax external messaging review  
• Management awareness of tax exposures  
• Transfer pricing policy review |
## Hot Topic Areas

<table>
<thead>
<tr>
<th>Audit Plan Hot Spot</th>
<th>Basic Controls Discipline</th>
<th>Risks</th>
<th>Recommended Actions</th>
</tr>
</thead>
</table>
| 5: Basic Operating Controls | • Employee turnover affecting control ownership  
                           |   • Adverse control impact of organizational realignment  
                           |   • Cost-reduction pressure  
                           | • Emerging markets expansion risk  
                           |   • Knowledge management risk  
                           |   • Change management risk  
                           |   • Regulatory risk  
                           | • Product or service offering reviews  
                           |   • Evaluation of reengineered business processes  
                           |   • Governance review audits  
                           |   • Process maturity assessment |
| 6: Project Management     | • Mismanagement of project portfolios  
                           |   • Insufficient project management expertise  
                           |   • Inadequate monitoring of realized project benefits  
                           | • Project failure  
                           |   • Financial loss  
                           |   • Product launch delays  
                           |   • Failed systems implementation  
                           | • Project resource planning review  
                           |   • Project benefits realization assessment  
                           |   • Project health checks  
                           |   • Project manager effectiveness review |
### Hot Topic Areas

<table>
<thead>
<tr>
<th>Audit Plan Hot Spot</th>
<th>Basic Controls Discipline</th>
<th>Risks</th>
<th>Recommended Actions</th>
</tr>
</thead>
</table>
| **7: Third-Party Relationships** | • Stronger supply chain vulnerability  
                              • Increased reliance on third parties to perform core business roles  
                              • Intensified regulatory focus on third-party relationships | • Reputation risk  
                              • Poor or inconsistent quality  
                              • Data access risks  
                              • Compliance risk | • Third-party governance review  
                              • Audit rights review  
                              • Due diligence in selecting third-party relationships  
                              • Supplier chain management health check |
| **8: Talent Management**  | • Talent shortages  
                              • Talent attrition and succession planning risk  
                              • Low employee engagement | • Hampered business growth  
                              • Leadership deficit  
                              • Poor knowledge management | • Critical positions review  
                              • Knowledge management audit  
                              • Retention effectiveness review  
                              • Career development program review  
                              • Hiring practices review |
### Hot Topic Areas

#### Audit Plan Hot Spot	Basic Controls Discipline	Risks	Recommended Actions
---
9: Tone at the Middle
- Middle managers receive most reports of alleged misconduct
- Middle managers disproportionately affect employee behaviors
- The tone at the top does not always trickle down
- Inadequate tone at the top
- Emerging markets risk
- Whistleblower programs
- Fraudulent activities
- Tone at the middle review
- Manager training audit
- Measurement and reward check
- Whistleblower program audit

10: Reputation Risk
- Instantaneous transparency
- Rapidly shifting stakeholder expectations
- Hyper-connectedness
- Market value decline
- Customer retention
- Investor management
- Weakened brand
- Stakeholder expectations and brand perceptions review
- Internal communications review
- Corporate communications audit
- Training review
Key Takeaways

✓ FACT. Senior management commitment to strong internal control is the number one (#1) factor to a strong control environment. The tone for what is acceptable is set at the top.
✓ FACT. Internal controls are *key* to preventing or detecting fraud and are essential for all organizations.
✓ FICTION. Good controls will always remain good controls.
✓ FACT. If your company hasn’t examined their internal controls in the past two years or passes certain milestones, it’s time to update them.
✓ FACT. Segregation of duties (SOD) is a critical element of internal controls.
✓ FICTION: SOD controls are IT controls and should be managed by the technology team.
✓ FACT. Good controls reduce the exposures inherent with the current economic environment.
✓ FACT. Good controls allow scalable and controlled organization growth.
✓ FICTION. A risk assessment is sufficient for establishing strong internal controls.
✓ FACT. Segregation (separation) of duties (SOD) is a critical element of internal controls.
✓ FACT. Good controls increase the operational effectiveness of your organization by detecting errors and reducing rework.
Moss Adams is a fully integrated professional services firm dedicated to personally assisting clients with growing, managing, and protecting prosperity. With more than 2,600 professionals across over 20 locations in the West and beyond, we work with many of the world’s most innovative companies and leaders.

Colin Wallace, Partner – Advisory Services
(972) 924-5089
(503) 309-4593
colin.wallace@mossadams.com