Compliance and Internal Audit:
Working together to identify and remEDIATE controls in compliance risk areas

Sheryl Vacca, CCEP-F, CCEP-I
SVP/Chief Compliance & Audit Officer
University of California
Sheryl.vacca@ucop.edu

Odell Guyton
Director of Compliance
Microsoft Corporation

Agenda

- Governance Framework
- Importance of Strong Ethics and Values
- IA and Compliance Organizations
- IA and Compliance Culture of Compliance
- IA and Compliance Collaborations

What is Governance?

“Corporate governance is the policies, processes, structures, and controls used within an organization by all involved (Board of Directors, management, auditors, and employees) to achieve its objectives in an ethical manner.”

- Institute of Internal Auditors
Key Elements for an Effective Program
Across Industries have been identified
Globally these standards have been introduced:
- Purpose is to prevent and detect violations of law, regulations, policies, guidelines, etc. for which the organization is, or would be, liable
In evaluating compliance programs, prosecutors may consider whether the corporation has established corporate governance mechanisms that can effectively detect and prevent misconduct. ...do the corporation’s directors exercise independent review over proposed corporate actions rather than unquestioningly ratifying officers’ recommendations; are the directors provided with information sufficient to enable the exercise of independent judgment, are internal audit functions conducted at a level sufficient to ensure their independence and accuracy and have the directors established an information and reporting system in the organization reasonable designed to provide management and the board of directors with timely and accurate information sufficient to allow them to reach an informed decision regarding the organization’s compliance with the law. In re: Caremark, 698 A.2d 959 (Del. Ct. Chan. 1996).

Effective Compliance

- Establish Standards: Establish standards and procedures to prevent and detect criminal conduct
- Set Examples: High-level personnel of the organization shall ensure that the organization has an effective compliance and ethics program
- Management Integrity: Exercise due diligence and not place individuals with questionable backgrounds into positions of substantial authority
- Communicate and Train: Communicate the standards and procedures of its compliance and ethics program to all employees and conduct effective ethics training programs
- Prevent and Detect: Ensure its compliance and ethics program is followed, evaluates the effectiveness of its program, and publicize a confidential system for the reporting of suspected wrongdoing
- Promote and Enforce: Promote and enforce compliance and ethics program consistently throughout the organization
- Assess and Respond: Take reasonable steps to respond appropriately to criminal conduct
Changing Business Environment: Scrutiny In All Corners of the World

- U.S. and Global Environment – Public Demand for Corporate Governance
  - US Federal Sentencing Guidelines
  - Sarbanes-Oxley Requirements
  - NASDAQ Listing Requirements
  - SEC Regulations
  - State Attorneys General
  - Responsible Business Practices
- Board of Directors Accountability
- CEO-CFO Accountability
- Management Accountability
  - Culture of Compliance / Tone at the Top
- Investor Confidence

Recent Cases
- Walmart
- Petrobras
- Embraer
- Biomet
- Volkswagen
- Louis Berger
- GlaxoSmithKline (GSK)
- Pfizer

Organizational controls – commonly missing or not working

- Failure of Leadership & A Culture of Corruption
- Organizational Weaknesses
- Absence of an Effective Internal Audit Department
- A Board of Directors in the Dark
- Lack of an Effective Compliance Program

Compliance Charter - Example

- Compliance High Level Oversight
  - Chief Compliance Officer
  - Director of Compliance

Promote Culture of Accountability
- Inform Organization’s Global Leadership
- Engage Management in Compliance Activities
- Prepare Reports to Audit Committee of the Board
- Participate in Fraud Disclosure Process
- Certification Process for employees (internal)
- Collaborate with Auditors to develop systemic compliance programs
- Establish metrics that encourage consistency, accountability

Meet or Exceed Government Standards and Industry Practice
- Standards of Business Conduct
- Risk Management
- Global Compliance Training & Awareness Communications
- Investigations Management and Policy Guidance
- Business Conduct Line & Reporting
- Non-Negotiables
- Obeying The Law
- Microsoft Policies

Corporate Values
- Integrity & Honesty
- Open & Respectful
- Big Challenges
- Passion
- Accountable
- Self-Critical

Non-Negotiables
- Obeying The Law
- Compliance
- Microsoft Policies

Code of Conduct – increasing “awareness” and defining “expectations”

Standards of Business Conduct – All employees, directors, and officers worldwide

Finance Code of Professional Conduct – CEO, CFO and all Finance employees

Vendor Code of Conduct – All VP and Vendors

Policy for Compliance Conduct Standards

Non-Negotiables
- Obeying The Law
- Compliance
- Microsoft Policies
Internal Audit
• Highlight and document areas of non-compliance which can clarify and better communicate policies or tighten enforcement. Prevent and ensure that the compliance program is effectively adopted and seen as viable to instances of potential fraud which was dealt with outside the Investigative Framework. Evaluate the implementation of the organization's ethics-related objectives, programs, and activities.

Compliance
• Collaborate to identify regulatory requirements, compliance risks and understand the requirements, roles, and responsibilities.
• Engage with business to develop compliance plans with:
  • Clear ownership
  • Documented business processes
  • Ongoing monitoring and process improvement
  • Legal and compliance training and awareness
  • Investigation and Response
  • Consistent Discipline

**Governance**

**Importance of Strong Ethics and Values**

**IA and Compliance**

**Culture of Compliance**

**Collaborations**

**Synergies between IA and Compliance**

**Fraud Prevention Culture** - example

**THE GOAL:** Taking fraud prevention and business ethics from a compliance initiative to a cultural mindset

**Shared Investigative Resource Model**

**FINANCIAL INTEGRITY WorkTeam**

Clear and common understanding of fraud prevention requirements and the role of management

**Culture of Compliance**

**Internal Audit**

**Compliance**

**Financial Integrity WorkTeam**

**Management Control**

**Common Definition of Fraud and Understanding of Responsibilities**
Financial Integrity Work Team-example

- Staff with professionally trained & experienced fraud investigators and Certified Fraud Examiners
- Based in internal audit with a worldwide charter
- Maintain close alignment with executive leadership, Internal Audit, Finance, Legal, Compliance, HR, corporate security and other entity organizations
- Operate under the legal guidance of the Compliance and local Legal and Corporate Affairs
- Responsible for the detection, investigation & prevention of fraud & abuse & recovery of assets
- Coordinate investigative activities with Internal Audit and the Controller community to ensure that investigative results are considered by the appropriate committee
- Emphasize on fraud awareness and prevention throughout the Company

Example of collaboration between financial controls and compliance

IA-Compliance Interface

Detection
- Compliance Program
- Fraud Risk Assessment
- Fraud Auditing
- Hotline

Investigation
- Data Collection Analysis
- Investigation Technique
- Interview Reporting

Prevention
- NEO
- NMO
- Training and Communication
- Background Checks
- Code of Conduct

Resolution
- Recovery
- Restitution
- Prosecution
- Cost Efficacy
- Process Improvements

Benefits of IA/Compliance Collaboration

- IA/Compliance- Association between the two makes each better
- Mutually supportive
- Close coordination and cooperation are hallmarks

Ensures a strong governance foundation and structure

IA evaluates Compliance program (IA Standards)
Developing Roles of IA-Compliance Collaborative Effort - examples

- Creation of financial controls to develop fraud prevention, detection and investigation capabilities done jointly
- Conduct annual overall fraud risk assessments
- Perform Fraud and Standard of Business Conduct risk assessments and procedures
- Perform overall corporate compliance program reviews and detailed audits of specific program aspects
  - e.g., Employee background check process
- Quarterly external financial reporting audits, with focus on significant estimates and disclosure processes
- Quarterly spend abuse audits
- Continuous Control Monitoring (CCM) reviews by management
- Vendor compliance audits

What is next?

- Further alignment of risk assessment and compliance monitoring
- Enhance productivity of collaboration and bring other parts of compliance community into the same level of collaboration
- Net effect of strong collaboration between internal audit and compliance results in and enhances governance, culture of compliance, and the performance and effectiveness of both organizations

QUESTIONS

Sheryl.vacca@ucop.edu