Compliance Assurance

Higher Education – Compliance Conference
June 6, 2016
12:30 pm – 2 pm

Urton Anderson, CCEP
Director of the Von Allmen School of Accountancy and EY Professor
The University of Kentucky

Mark Salamasick
Executive Director Audit-Academic
University of Texas System

Session Objectives

- Understand management and the board’s needs for compliance assurance
- Learn techniques to develop more effective and efficient monitoring and auditing plans
- Exchange insights and best practices for obtaining assurance on compliance
Session Agenda

- Compliance Assurance?
- Role of Compliance Assurance in Organizational Governance
  - The Governance Process
    - Board and its role in compliance
    - Management and its role in compliance
- Monitoring Activities and the Three Lines of Defense
- Developing Effective Monitoring Plans and Strategies
- Providing Effective Assurance
- The Future of Compliance Assurance
  - Combined Assurance
  - Assessing Assurance Providers
  - Maturity Model for Assurance

Compliance Assurance

Auditing and monitoring activities to provide assurance that compliance risks are within the organization’s risk appetite

Provide Assurance to:

- Board
- Management
http://www.youtube.com/watch?v=As6y5eI01XE

Rising Demand for Compliance Assurance

Factors Increasing Complexity of the Legal and Regulatory Environment

- Technological Advancements
- Globalization
- Increased Interdependency of Organizations
- Demand for Accountability
ROLE OF COMPLIANCE ASSURANCE IN ORGANIZATIONAL GOVERNANCE

What is organizational governance?

The process through which
(1) values and goals are established and communicated,
(2) the accomplishment of goals is monitored,
(3) accountability is ensured, and
(4) values are preserved.
The Two Basic Responsibilities of the Board

- Values
- Objectives
- Boundaries

Governance "Umbrella"
Board of Directors

Strategic Direction

Governance Oversight

- Accountability
- Values preservation

Key Components of Governance Oversight

Governance Umbrella
Board of Directors

Stakeholders

Risk Management
Senior Management
Risk Owners

Assurance
Internal ↔ External
**Parties in the Governance Process**

- **Oversight group** – board and committees of the board
- **Stewardship group** – executive management
  - Dual role of stewardship of resources allocated by board and accountability of results of operations
- **Performance group** – operating and support management and staff
- **Assurance group** – internal and external auditing functions
  - and in some organizations - compliance.

**Board’s Role in Compliance**

2) (A) The organization’s governing authority shall be knowledgeable about the content and operation of the compliance and ethics program and shall exercise reasonable oversight with respect to the implementation and effectiveness of the compliance and ethics program.

*Fed. Sent. Guidelines Chapter 8*
**Reasonable Oversight**

A director has a duty to attempt in good faith to assure that

1. a corporate information and reporting system exists, and

2. this reporting system is adequate to assure the board that appropriate information as to compliance with applicable laws will come to its attention in a timely manner as a matter of ordinary operations.


**The Management’s Role in Compliance**
Management’s Responsibility

To ensure that all operations are conducted in accordance with applicable law, regulations and policies, including internal policies.

Compliance Programs are designed to establish a culture within an organization that promotes prevention, detection and resolution of instances of conduct that do not conform to federal and state law, as well as the organization’s ethical and operations policies.

Management’s Responsibility

Internal Control – COSO Model
Internal Control

...a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations.
- Reliability of financial reporting.
- Compliance with applicable laws and regulations.

COSO

Compliance as a Goal
Federal Sentencing Criteria for effective compliance program – 7 minimal requirements

#5. The organization shall take reasonable steps—
(A) to ensure that the organization’s compliance and ethics program is followed, including monitoring and auditing to detect criminal conduct;
(B) to evaluate periodically the effectiveness of the organization’s compliance and ethics program; and
(C) to have and publicize a system, which may include mechanisms that allow for anonymity or confidentiality, whereby the organization’s employees and agents may report or seek guidance regarding potential or actual criminal conduct without fear of retaliation.

Hallmarks of Effective Compliance Programs

- Commitment from Senior Management and a Clearly Articulated Policy Against Corruption
- Code of Conduct and Compliance Policies and Procedures
- Oversight, Autonomy, and Resources
- Risk Assessment
- Training and Continuing Advice
- Incentives and Disciplinary Measures
- Third-Party Due Diligence and Payments
- **Confidential Reporting and Internal Continuous Improvement: Periodic Testing and Review**
- Mergers and Acquisitions: Pre-Acquisition Due Diligence and Post-Acquisition Integration

SEC and DOJ – Hallmarks of Effective Program

Finally, a good compliance program should constantly evolve. A company’s business changes over time, as do the environments in which it operates, the nature of its customers, the laws that govern its actions, and the standards of its industry. In addition, compliance programs that do not just exist on paper but are followed in practice will inevitably uncover compliance weaknesses and require enhancements. Consequently, DOJ and SEC evaluate whether companies regularly review and improve their compliance programs and not allow them to become stale.

…An organization should take the time to review and test its controls, and it should think critically about its potential weaknesses and risk areas. … DOJ and SEC will give meaningful credit to thoughtful efforts to create a sustainable compliance program if a problem is later discovered.

Practice Advisory 2050-2 - Assurance Maps

- One of the key responsibilities of the board is to gain assurance that processes are operating within the parameters it has established to achieve the defined objectives.
- It is necessary to determine whether risk management processes are working effectively and whether key or business-critical risks are being managed to an acceptable level.
MONITORING ACTIVITIES AND THE THREE LINES OF DEFENSE

Why Monitor?
Internal Control

Compliance as a Goal

...a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations.
- Reliability of financial reporting.
- Compliance with applicable laws and regulations.

COSO

Monitoring and Auditing

- A process that assesses the quality of the internal control system's performance over time

Monitoring

Auditing
Monitoring Activities

- Line management and employees (management provides assurance as a first line of defense over the risks and controls for which they are responsible.) – Supervisory controls
- Senior management – Oversight controls
- Internal and external auditors
- Compliance
- Quality assurance
- Risk management
- Environmental auditors
- Workplace health and safety auditors
- Government performance auditors
- Financial reporting review teams
- External financial statement auditors
- Other external assurance providers, including surveys, specialist reviews (health and safety), etc.

Organization as a Web of Assurance
Assurance Network

- Information security
- Human capital
- FCI compliance
- Line management
- Internal audit
- External audit
- Ethics and integrity
- Business risk management
- Compliance

**Board**
- Board audit committee
- Executive committee
- Compensation committee
- Risk committee
- Governance committee
- Finance committee

**Management Committees**
- Risk management
- Liquidity management committee
- Compliance leadership teams
- SOX compliance committees
- Various business units
- Quality system
- ISO
- Insurance
- Environmental
- Security

Assurance Fatigue
Business Unit 1– Monitoring Schedule

<table>
<thead>
<tr>
<th>Business Unit 1 – Monitoring Schedule</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assurers</td>
</tr>
<tr>
<td>Internal Audit</td>
</tr>
<tr>
<td>Compliance</td>
</tr>
<tr>
<td>FCPA</td>
</tr>
<tr>
<td>SOX</td>
</tr>
<tr>
<td>EH&amp;S</td>
</tr>
<tr>
<td>Risk Management</td>
</tr>
<tr>
<td>Info Security</td>
</tr>
<tr>
<td>Fraud</td>
</tr>
<tr>
<td>External Audit</td>
</tr>
</tbody>
</table>

Standard 2050 (Proposed change)

Coordination and Reliance
The chief audit executive should share information and coordinate activities with other internal and external providers of assurance and consulting services providers to ensure proper coverage and minimize duplication of efforts.

Interpretation
In coordinating activities, the chief audit executive may rely on the work of other assurance and consulting service providers. A consistent process for the basis of reliance should be established, and the chief audit executive should consider the competency, objectivity, and due professional care of the assurance and consulting service providers. The chief audit executive should also have a clear understanding of the scope, objectives, and results of the work performed by other providers of assurance and consulting services. Where reliance is placed on the work of others, the chief audit executive is still accountable and responsible for ensuring adequate support for conclusions and opinions reached by the internal audit activity.
3 Lines of Defense

Basel II - Basel Committee on Banking Supervision, UK, ECIIA

The Three Lines of Defense Model

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Controls</td>
<td>Financial Control</td>
<td>Internal Audit</td>
</tr>
<tr>
<td>Internal Control Measures</td>
<td>Security</td>
<td>Compliance</td>
</tr>
<tr>
<td></td>
<td>Risk Management</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Quality</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Inspection</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Compliance</td>
<td></td>
</tr>
</tbody>
</table>

Governing Body / Board / Audit Committee

Senior Management

Regulator

External audit

Line 1
Management oversight - management review, control self-assessment, and continuous monitoring mechanisms

Line 2
Staff functions – Risk management, SOX review, compliance

Line 3
Independent and objective assurance – IA, EA, ISO, regulatory audits and other impendent reviews

Basel II - Basel Committee on Banking Supervision, UK, ECIIA
Guidance

Deciding who is on Point for Compliance-Audit or Compliance

- Scholarship Processing
- Communications
- Compliance with Laws/Policies and Procedures
- Student/Donor Relations
How best to describe compliance and audit?

Developing Effective Monitoring Plans and Strategies

1. Risk Assessment
2. Prioritize Risks
3. For High Risk Develop Monitoring Plan
4. Implement
5. Assess Effectiveness (i.e., Audit)
(1) Start with Compliance Risk Assessment

Compliance Risk Assessment Options

1. Organizations ERM
2. Separate Compliance Risk Assessment
3. With Internal Audit Risk Assessment
(2) Prioritize Risks

- Scoring Method
- Focus on Highest Risk
- Clear Understanding of Ownership
- Make sure Projects and Initiatives are Included

(3) Designing Monitoring and Auditing Plan

<table>
<thead>
<tr>
<th>Risk</th>
<th>Risk Owner</th>
<th>Risk Rating (H,M,L)</th>
<th>1st Line</th>
<th>2nd Line</th>
<th>3rd Line</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Operating Controls</td>
<td>Supervisory</td>
<td>Oversight</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
4. Assess Effectiveness

The Three Lines of Defense Model

1st Line of Defense: Management Controls, Internal Control Measures
3rd Line of Defense: Internal Audit

PROVIDING EFFECTIVE ASSURANCE
Auditing Compliance System Effectiveness

Part 1 – Evaluating the effectiveness of controls specifically designed to reduce the risk of noncompliance in the high risk areas identified by the organization’s risk assessment process.

Part 2 - The assessment of the overall effectiveness of the compliance program which at a minimum would include evaluating the organization’s process for assessing risk of noncompliance and ethical misconduct and the design and implementation of Seven Elements.
THE FUTURE OF COMPLIANCE ASSURANCE

- Combined Assurance
- Assessing Assurance Providers
- Maturity Model for Assurance

COMBINED ASSURANCE

COMBINED ASSURANCE
King III
Principle 3.5
The audit committee should ensure that a combined assurance model is applied to provide a coordinated approach to all assurance activities.
Implementing combined assurance is not something that can be achieved from one day to the next—it should be considered a journey.

—Marie-Helene Laimay, CAE, Sanofi, France
Implementation of Combined Assurance

Knowledge and implementation of the combined assurance concept is not yet widespread.

The lowest level of implementation is in North America at 25% and the highest is in South Asia and Sub-Saharan Africa (around 50%).

---

Assessing Assurance Providers

How is assurance provided

<table>
<thead>
<tr>
<th>Assurance Provider</th>
<th>Health &amp; Safety (H&amp;S)</th>
</tr>
</thead>
<tbody>
<tr>
<td>How is assurance provided</td>
<td>Self assessment</td>
</tr>
<tr>
<td></td>
<td>Incident tracking and remediation</td>
</tr>
<tr>
<td></td>
<td>H&amp;S analysis and reporting</td>
</tr>
<tr>
<td>How is assurance measured</td>
<td>Number and scores of self assessments performed</td>
</tr>
<tr>
<td></td>
<td>Number of BUs ISO 14001 certified</td>
</tr>
<tr>
<td></td>
<td>Number of OHSAS pre-audits performed</td>
</tr>
<tr>
<td></td>
<td>Number of recommendations made to CEOs for improvement</td>
</tr>
</tbody>
</table>
Five Principles in Determining Reliance

1. Purpose
2. Independence and Objectivity
3. Competence
4. Elements of Practice
5. Communication of Results & Impactful Remediation

Assurance Reliance

IPPF – Practice Guide Reliance by Internal Audit on Other Assurance Providers – December 2011
Assurance Maturity Model

Assurance Maturity Curve

Questions?

Urton Anderson
Von Allmen School of Accountancy
The University of Kentucky
(859)218-1788
urton.anderson@uky.edu

Mark Salamasick
Executive Director of Audit – Academic
The University of Texas System
(512) 499-4535
msalamasick@utsystem.edu