Compliance and the 3 Lines of Defense

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

Session Agenda

- Assurance and Risk Management in Organizational Governance
  - The Demand for Assurance
- Organization as an Assurance Network
- 3 Lines of Defense Model and Compliance
  - What is the 3 Lines of Defense model?
  - Why implement a line of defense approach?
  - Who are the players in each line?
  - What are the risks and dependencies of each line?
  - How do the three lines coordinate and collaborate?
- The Future – 3 Lines of Defense and Combined Assurance

Assurance and Risk Management in Organizational Governance

- The Continual Crisis in Organizational Governance
  - 1980s – S&L
  - 2002 – Enron et al.
  - 2007 – Global Financial Meltdown
  - VW, Wells Fargo, Uber, ???
Assurance and Risk Management in Organizational Governance

- Risk Management and Governance Oversight as Solution
  - Board Accountability
  - Executive Management Accountability

- Demand for Assurance

Rising Demand for Compliance Assurance

Factors Increasing Complexity of the Legal and Regulatory Environment

- Technological Advancements
- Globalization
- Increased Interdependency of Organizations
- Demand for Accountability

The 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.


---

Reasonable Oversight

- The Board should ensure that management and the Board have strong processes for identifying risk areas.
- The Board should ensure that management consistently reviews and audits risk areas, as well as develops, implements, and monitors corrective action plans.

---

The Executive Management's Role in Compliance

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.
Organization as a Web of Assurance

Sources of Assurance

- Line management and employees (management provides assurance as a first line of defense over the risks and controls for which they are responsible.)
- Senior management
- 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.
Organizations should define the interrelationship of the audit, compliance, and legal functions in charters or other organizational documents. The structure, reporting relationships, and interaction of these and other functions (e.g., quality, risk management, and human resources) should be included as departmental roles and responsibilities are defined.
What is the 3 Lines of Defense model?

3 Lines of Defense model distinguishes among three groups (or lines) involved in effective risk management—functions that:

- Own and manage (operating management)
- Oversee (risk, quality, and compliance functions)
- Provide independent assurance (internal audit)
Why implement a line of defense approach?

- Variety and complexity of risks rising rapidly
- Role clarification
- AC and other governing bodies need to know:
  - Someone in the organization is looking out for each risk area
  - Risk responsible people are working together to avoid gaps in risk management or duplication of efforts

Each area within the company needs a clearly defined and specific role. Helps reduce likelihood a risk will slip past all defense lines and impact the organization.

Who are the players in each line?

1st Line of Defense
- Responsible for managing risks and maintaining effective internal controls
- Identifies, assesses, mitigates, monitors and reports on risks
- Bottom Up Risk Assessments include:
  - Risk Control Self Assessment (RCSA)
  - Key Risk Indicators (KRI’s)
  - Risk Profile
  - Escalation
1st Line of Defense

- Operational Controls
- Monitoring Controls

2nd Line of Defense

- Designs and implements risk program
- Provides framework used by 1st line to assess and manage risk
- Connects dots by taking a portfolio view of risks across the enterprise
- Coordinates risk governance process
- Provides compliance function to monitor various specific risks
- Provides top down view relative to strategy and risk appetite

Examples
- Compliance
- Legal
- Financial control
- Security
- Risk management
- Quality
- Health and safety
- Inspection
- Environmental
- Supply chain
3rd Line of Defense

- Internal Audit has been clearly defined as the Third Line of Defense by the IIA, COSO 2013, regulators, and other published guidance

- 3rd Line has to be fully independent and objective

Compliance as a 3rd line

What is necessary?

Safeguards

- Discussion with board
- Acceptance and ownership of risk by management
- Clear definition and assignment of roles for each activity where 2nd and 3rd roles overlap
  - Impact and risk to compliance and organization
  - Roles, responsibilities, and segregation of duties
  - Period evaluation of independence objectivity of assurance activities

Compliance Example

Conflict of Interest
### Compliance Example

<table>
<thead>
<tr>
<th>Role Area</th>
<th>1st Line</th>
<th>2nd Line</th>
<th>3rd Line</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do I Identified During Risk Assessment?</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Complies with performance</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Reports external</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Reports internal</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Do I Identified During Risk Assessment?</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Compliance Officer Important</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Do I Identified During Risk Assessment?</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Do I Identified During Risk Assessment?</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Additional Roles in the Model

**Tone at the Top**
- Governing body/Board/Audit Committee
- Senior management

**Responsible and accountable for setting objectives, defining strategies to achieve them, and establishing governance structures and processes to best manage risks in accomplishing those objectives**

**Key to effective implementation of Three Lines Model by setting tone and establishing and enforcing accountability**
The 4th Line of Defense

- External bodies that reside outside the organization’s structure but have an important role in overall governance and control structure
  - Regulators
  - External Auditors
  - SEC
  - Etc.
- Often influence control environment and expect a higher level of expectation
- May often audit/examine 1st, 2nd and 3rd lines
- Yet another line of defense for the organization’s stakeholders, including the Board and senior management

What are the risks and dependencies of each line?

Additional Roles in the Model

The “4th” Line

1. External bodies that reside outside the organization’s structure but have an important role in overall governance and control structure
   - Regulators
   - External Auditors
   - SEC
   - Etc.
   - Often influence control environment and expect a higher level of expectation
   - May often audit/examine 1st, 2nd and 3rd lines
   - Yet another line of defense for the organization’s stakeholders, including the Board and senior management
How do the three lines coordinate and collaborate?

- Risk and control processes should be structured in accordance with the Three Lines of Defense model.
- Each line should be supported by appropriate policies and role definitions.
- Defining roles and responsibilities is key.
- Proper coordination and communication should occur among lines to foster efficiency and effectiveness.
- Lines of defense should not be combined or coordinated in a manner that compromises their effectiveness.
- When functions at different lines are combined, the governing body should be advised of the structure and its impact.

The Future – 3 Lines of Defense and 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.
Combined Assurance Benefits

- Provides Board/Governance Body and senior management with assurance needed to carry out their responsibilities

- Reduce “assurance fatigue”

Assurance Map (PWC)

Implementing

- Step 1: Establishing the business case
- Step 2: Assurance reality check – what risk, source of assurance, how
- Step 3: Risk mapping
- Step 4: Combined assurance design
- Step 5: Implement
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%).
Questions?

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