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, ???

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.
## Business Unit 1– Monitoring Schedule

<table>
<thead>
<tr>
<th>Assurers</th>
<th>J</th>
<th>F</th>
<th>M</th>
<th>A</th>
<th>M</th>
<th>J</th>
<th>Ju</th>
<th>A</th>
<th>S</th>
<th>O</th>
<th>N</th>
<th>D</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal Audit</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Compliance</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>FCPA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SOX</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EH&amp;S</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Risk Management</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Info Security</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fraud</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>External Audit</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Assurance Fatigue
Role Clarification

- 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.

3 Lines of Defense Model and Compliance
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)

3 Lines of Defense Model

Basel II - Basel Committee on Banking Supervision, UK, ECIIA
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
- Management Controls
- Internal Control Measures
- Identify, Assess, Monitor & Elevate Possible Risk Events
Front Line

2nd Line of Defense
- Financial Control
- Security
- Enterprise Risk Management
- Credit Management
- Appraisal
- Compliance
Middle Office

3rd Line of Defense
- Internal Audit

Governing Body / Board / Audit Committee
Senior Management
Regulator
External Audit
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

---

3rd Line of Defense

- 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

<table>
<thead>
<tr>
<th>Risk Area</th>
<th>1st Line</th>
<th>2nd Line</th>
<th>3rd Line</th>
</tr>
</thead>
<tbody>
<tr>
<td>As Identified During Risk Assessment</td>
<td>What do the units do to help mitigate this risk?</td>
<td>What do you monitor to help mitigate this risk?</td>
<td>What type of audits exist to help mitigate this risk?</td>
</tr>
<tr>
<td>Conflict of Interest</td>
<td>- Educate personnel about COI policies.</td>
<td>- Open Payments database</td>
<td>- 10% of outside travel payments against Accounts Payable travel</td>
</tr>
<tr>
<td></td>
<td>- Report non-compliance to COI Manager.</td>
<td>- Annual COI disclosure</td>
<td>reimbursements.</td>
</tr>
<tr>
<td></td>
<td>- Report unauthorized vendors representatives and displays</td>
<td>- Purchasing and Pharmacy vendor registrations.</td>
<td>- Level 2 review of COI disclosures</td>
</tr>
<tr>
<td></td>
<td>- Advise personnel to contact Compliance with questions</td>
<td>- Research conflict database cross-check</td>
<td>- 10% of &quot;nothing to disclose&quot;</td>
</tr>
</tbody>
</table>

### Compliance Example

<table>
<thead>
<tr>
<th>Risk Area</th>
<th>1st Line</th>
<th>2nd Line</th>
<th>3rd Line</th>
</tr>
</thead>
<tbody>
<tr>
<td>As Identified During Risk Assessment</td>
<td>What do the units do to help mitigate this risk?</td>
<td>What do you monitor to help mitigate this risk?</td>
<td>What type of audits exist to help mitigate this risk?</td>
</tr>
<tr>
<td>Gifts/Industry influence</td>
<td>- Report vendors who are onsite without permission</td>
<td>- Open Payments Database</td>
<td>- Conflict Management Plan</td>
</tr>
<tr>
<td></td>
<td>- Educate staff to not accept gifts</td>
<td>- Annual disclosure review</td>
<td>- Data trends analysis</td>
</tr>
<tr>
<td>Reconciliation of payments for</td>
<td>- Follow business procedures to receive outside moneys for contractual</td>
<td>- Tier 2 investigations</td>
<td>- Develop strategy for on-site evaluation at contractual</td>
</tr>
<tr>
<td>contractual agreements</td>
<td>obligations</td>
<td>- Recommendations to Conflict Committee</td>
<td>locations</td>
</tr>
<tr>
<td>Research misconduct</td>
<td>- Office of Research Integrity monitors data, receives and investigates</td>
<td>- Request and review monthly report for outside payments made to faculty</td>
<td></td>
</tr>
<tr>
<td></td>
<td>reports</td>
<td>- Spot-check contractual terms</td>
<td></td>
</tr>
<tr>
<td>Undisclosed family relationships</td>
<td>- Notify Compliance of family relationships</td>
<td>- Ask dept for more information</td>
<td></td>
</tr>
<tr>
<td>Consistency of corrective actions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>for faculty – financial, reputational</td>
<td></td>
<td></td>
<td></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
**Additional Roles in the Model**

- **The 4th Line**

  - 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?

Financial Service Industry Example
### How do the three lines coordinate and collaborate?

- Risk and control processes should be structured in accordance with 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

### Risk Assurance Map – Starting Template

<table>
<thead>
<tr>
<th>Provider Assessment</th>
<th>Overall Provision</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low Assurance</td>
<td>Opportunity to Remove / Refocus Effort</td>
</tr>
<tr>
<td>Medium Assurance</td>
<td>Maintain Current Status</td>
</tr>
<tr>
<td>High Assurance</td>
<td>Assurance Gap</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Asset Safeguarding</th>
<th>...</th>
<th>...</th>
<th>...</th>
<th>...</th>
</tr>
</thead>
<tbody>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Management 1st Line</th>
<th>Functional Oversight 2nd Line</th>
<th>Independent 3rd Line</th>
<th>Regulatory Oversight 4th Line</th>
<th>Corrective Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Asset Safeguarding</th>
<th>...</th>
<th>...</th>
<th>...</th>
<th>...</th>
</tr>
</thead>
<tbody>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>
### BU Risk Assurance Map – Illustrative Example

#### Risk Universe

<table>
<thead>
<tr>
<th>Strategic Risks</th>
<th>External</th>
<th>Internal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change in Laws/Regulations</td>
<td>-</td>
<td>N/A</td>
</tr>
<tr>
<td>Competitor</td>
<td>-</td>
<td>N/A</td>
</tr>
<tr>
<td>Economic</td>
<td>-</td>
<td>N/A</td>
</tr>
<tr>
<td>Industry</td>
<td>-</td>
<td>N/A</td>
</tr>
<tr>
<td>Reputation</td>
<td>-</td>
<td>N/A</td>
</tr>
<tr>
<td>Stakeholder</td>
<td>-</td>
<td>N/A</td>
</tr>
<tr>
<td>Technology</td>
<td>-</td>
<td>N/A</td>
</tr>
<tr>
<td>Business Strategy</td>
<td>-</td>
<td>N/A</td>
</tr>
<tr>
<td>Customer Satisfaction</td>
<td>-</td>
<td>N/A</td>
</tr>
<tr>
<td>Goal Setting/Alignment</td>
<td>-</td>
<td>N/A</td>
</tr>
<tr>
<td>Governance</td>
<td>-</td>
<td>N/A</td>
</tr>
<tr>
<td>Market Intelligence</td>
<td>-</td>
<td>N/A</td>
</tr>
<tr>
<td>Pricing</td>
<td>-</td>
<td>N/A</td>
</tr>
<tr>
<td>Product/Service Failure</td>
<td>-</td>
<td>N/A</td>
</tr>
<tr>
<td>Resource Allocation</td>
<td>-</td>
<td>N/A</td>
</tr>
</tbody>
</table>

#### Implementation of Combined Assurance

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

- **40%** Implemented combined assurance model
- **29%** Not implemented, but plan to adopt one in the next 2 to 5 years
- **31%** Not implemented, and do not have plans to adopt one in the next 2 to 5 years

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

### Implementation

<table>
<thead>
<tr>
<th>Region</th>
<th>0%</th>
<th>20%</th>
<th>40%</th>
<th>60%</th>
<th>80%</th>
<th>100%</th>
</tr>
</thead>
<tbody>
<tr>
<td>South Asia</td>
<td>2%</td>
<td>7%</td>
<td>13%</td>
<td>17%</td>
<td>30%</td>
<td>47%</td>
</tr>
<tr>
<td>Sub-Saharan Africa</td>
<td>39%</td>
<td>12%</td>
<td>34%</td>
<td>15%</td>
<td>30%</td>
<td>47%</td>
</tr>
<tr>
<td>East Asia &amp; Pacific</td>
<td>36%</td>
<td>12%</td>
<td>25%</td>
<td>30%</td>
<td>30%</td>
<td>40%</td>
</tr>
<tr>
<td>Europe</td>
<td>54%</td>
<td>7%</td>
<td>28%</td>
<td>31%</td>
<td>31%</td>
<td>40%</td>
</tr>
<tr>
<td>Latin America &amp; Caribbean</td>
<td>30%</td>
<td>12%</td>
<td>33%</td>
<td>24%</td>
<td>28%</td>
<td>37%</td>
</tr>
<tr>
<td>Middle East &amp; North Africa</td>
<td>24%</td>
<td>10%</td>
<td>38%</td>
<td>28%</td>
<td>31%</td>
<td>37%</td>
</tr>
<tr>
<td>North America</td>
<td>21%</td>
<td>4%</td>
<td>26%</td>
<td>49%</td>
<td>58%</td>
<td>70%</td>
</tr>
<tr>
<td>Global Average</td>
<td>32%</td>
<td>8%</td>
<td>29%</td>
<td>31%</td>
<td>39%</td>
<td>50%</td>
</tr>
</tbody>
</table>

- Yes, implemented now
- Yes, but not yet approved by the board or audit committee
- No, but plan to adopt one in the next 2 to 3 years
- No, and do not have plans to adopt one in the next 2 to 3 years


### Questions?

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