Meeting Stakeholder Expectations for Assurance: Internal Audit’s Role in a Group Effort

Urton Anderson
The University of Texas at Austin
Agenda

- The IA Value Proposition
- The Demand for Assurance
- Assurance Mapping
- The Combined Assurance Approach
- Summary
The IA Value Proposition

Thesis

The fundamental value proposition for internal auditing is the role it plays in maintaining a system of effective 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 Governance Body of an Organization

- Governance “Umbrella”
- Board of Directors

- Strategic Direction
- Governance Oversight

- Values
- Objectives
- Boundaries

- Accountability
- Values preservation
Key Components of Governance Oversight

- Stakeholders
- Governance Umbrella (Board of Directors)
- Risk Management
  - Senior Management
  - Risk Owners
- Assurance
  - Internal
  - External
Governance

- **Strategic Direction**
  - Set boundaries
  - Set objectives
  - Establish values
  - Determine risk appetite

- **Oversight**
  - Risk management
  - Assurance
Depiction of Key Governance Elements
Internal Audit

- ...helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.
IA Customers

- Auditee
- Financial Management
- Audit Committee
- Vendors
- Senior Management
- External Auditors
- Regulators
- Suppliers

2/2/2012
What does the customer want?

Audit Committee/Board
- Safeguarding Assets
- Compliance with Laws and Regulations
- Reliability of Data

QUALITY OF INFORMATION

Operating Management
- Effectiveness and Efficiency of Operations
- Achievement of Organizational Objectives

CHANGE AGENT
The IA Value Proposition

Objectivity

Assurance

Insight
Internal auditing provides assurance on the organization’s governance, risk management, and control processes to help the organization achieve its strategic, operational, financial and compliance objectives.
OBJECTIVITY = Integrity, Accountability, & Independence

With commitment to integrity and accountability, internal auditing provides value to governing bodies and senior management as an objective source of independent advice.
VALUE PROPOSITION OF INTERNAL AUDITING

What STAKEHOLDERS should expect from your internal auditors
The Demand for Assurance

- Board

- Executive Management

Governance "Umbrella"
Board of Directors

Strategic Direction
- Values
- Objectives
- Boundaries

Governance Oversight
- Accountability
- Values preservation
Objectives

• Effectiveness and Efficiency of Operations

• Reliability of Financial Reporting and Safeguarding of Assets

• Compliance with Laws and Regulations
Responsibilities – Effectiveness & Efficiency?

- Board’s
- Executive Management
Responsibilities – Effectiveness & Efficiency?

Board’s

- **Reviewing and guiding corporate strategy, major plans of action, risk policy, annual budgets and business plans; setting performance objectives; monitoring implementation and corporate performance; and overseeing major capital expenditures, acquisitions and divestitures.**

  OECD Principles of Corporate Governance, 2004  
  (#1 of 8 responsibilities)

- Executive Management
Responsibilities – Reliability of Financial Reporting and Safeguarding of Assets?

- Board’s

- Executive Management
Responsibilities – Reliability of Financial Reporting and Safeguarding of Assets?

Board’s

- Ensuring the integrity of the corporation’s accounting and financial reporting systems, including the independent audit…

  OECD Principles of Corporate Governance, 2004
  (#1 of 8 responsibilities)

Executive Management

- SOX 302
Sky-rocketing 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.

The Executive 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.
Assurance Mapping

- Web of Assurance
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.
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.
3 Fundamental Classes of Assurance Providers

1. Those who report to management and/or are part of management (management assurance), including individuals who perform control self-assessments, quality auditors, environmental auditors, and other management-designated assurance personnel.

2. Those who report to the board, including internal audit, some cases compliance.

3. Those who report to external stakeholders (external audit assurance), which is a role traditionally fulfilled by the independent/statutory auditor.
Management Based Assurance

- Monitoring Function - Actions taken by management and others to assess the quality of internal control system performance over time
Assurance Continuum
(Levels of Control in COSO)

(Governance and Management Control Processes)

Periodic Assurance

(Governance Control Processes)

On-going Assurance

Management Control Processes

Level 4 Controls
(Internal Audit)

Level 1 Controls
(Execution)

Level 2 Controls
(Supervisory)

Level 3 Controls
(Oversight)

Level 4 Controls
(Internal Audit)

Pre-operations design review of on-going assurance

During execution of event or transaction

Immediately after execution of event or transaction

Soon after execution of event or transaction

Post-operations audit of execution of on-going assurance
Effective Monitoring

- Audit – level 4
- Oversight – level 3
- Supervisory – level 2
- Execution – level 1

Timeliness

Monitoring Controls
The Monitoring Function

- **Supervisory Controls**
  - Investigation of unusual items

- **Oversight Controls**
  - Customer surveys and complaint analysis

- **Auditing Controls**
  - Traditional internal audit
## Assurance Map

<table>
<thead>
<tr>
<th>Risk Category</th>
<th>Risk Owner</th>
<th>Inherent Risk Rating</th>
<th>Residual Risk Rating</th>
<th>Assurance - Supervisory</th>
<th>Assurance - Oversight</th>
<th>Assurance - Independent Mentoring</th>
<th>Assurance - Internal Audit</th>
<th>Assurance - External Provider</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<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>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<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>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# 3 Lines of Defense

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

<table>
<thead>
<tr>
<th>Line 1</th>
<th>Management oversight - management review, control self-assessment, and continuous monitoring mechanisms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Line 2</td>
<td>Staff functions – Risk management, SOX review, compliance</td>
</tr>
<tr>
<td>Line 3</td>
<td>Independent and objective assurance – IA, EA, ISO, regulatory audits and other impendent reviews</td>
</tr>
</tbody>
</table>
## Lines of Defense

<table>
<thead>
<tr>
<th>First line of defence</th>
<th>Second line of defence</th>
<th>Third line of defence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management oversight</td>
<td>Management of risk</td>
<td>Independent assurance</td>
</tr>
</tbody>
</table>

**Objective:** Setting strategy, performance measurement, and establishing and maintaining risk management, control and governance across the business.

**Reporting Lines:**
Executive Management Committees and Operational Committees providing direction, guidance and oversight over the focus areas.

**Assurance Providers:**
- Management
- Quality assurance functions
- Other: Project Management Office

<table>
<thead>
<tr>
<th>First line of defence</th>
<th>Second line of defence</th>
<th>Third line of defence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management oversight</td>
<td>Management of risk</td>
<td>Independent assurance</td>
</tr>
</tbody>
</table>

**Objective:** Providing a risk framework to improve decision making, planning and prioritisation of the business activities.

**Reporting Lines:**
- Risk Committees
- Compliance Committee
- Audit Committees
- Regulatory Forums, etc.

**Assurance Providers:**
- Risk: Risk Management, Regulatory Risk Management, Legal Risk Management,
- Other: Forensics, Consultancies within the business, e.g. Tax.

<table>
<thead>
<tr>
<th>First line of defence</th>
<th>Second line of defence</th>
<th>Third line of defence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management oversight</td>
<td>Management of risk</td>
<td>Independent assurance</td>
</tr>
</tbody>
</table>

**Objective:** Provides independent and objective assurance of the overall adequacy and effectiveness of governance, risk management and control within the organisation as established by the first and second layers of defence.

**Reporting Lines:**
- Regulators
- Board and Audit Committees.

**Assurance Providers:**
- Internal Audit
- External Audit/Advisors
- External regulators.
### 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>
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”
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
# Assurance Map (PWC)

## Processes

<table>
<thead>
<tr>
<th>Processes</th>
<th>First line of defence</th>
<th>Second line of defence</th>
<th>Third line of defence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management-based assurance</td>
<td>Control self assessment</td>
<td>Special project</td>
<td>Management review</td>
</tr>
<tr>
<td>Strategic</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cash/finance and treasury</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Funding</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sustainability</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Growth / mergers &amp; acquisitions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alliances</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operational</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Financial</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Treasury</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Human resources</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supply chain management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Quality</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Environment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customers</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Products &amp; services</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**IIA - Dallas Chapter**

**2/2/2012**
Summary

- New approach to assurance required
  - Increased demand for assurance
  - Assurance fatigue
- Map of the organization’s network of assurance
- Combined assurance approach
- New challenge for IA
CaE to CAE

- Responsibility of the CAE to understand the independent assurance requirements of the board and the organization, to clarify the role the internal audit activity fills and the level of assurance it provides.
Thank you!

Contact Information:
Urton Anderson
McCombs School of Business
The University of Texas at Austin
(512)471-5339 (messages until 8/1/12)
(202)551-5308 (until 7/31/12)
urton@mail.utexas.edu
Agenda

- IPPF
  - Code of Ethics
  - Standards