Combined Assurance: Holistic Assurance approach for Organization

Seminar Nasional Internal Audit
Lombok, 16 April 2014

Fandhy Haristha Siregar,
CIA, CISA, CISM, CISSP, CRMA, QIA, CEH, CEP-PM
Contents

• 3 Lines of Defense
• Assurance Providers
• Why Combined Assurance?
• Combined Assurance Approaches
• What are the Critical Success Factors?
• Combined Assurance: CIMB Niaga Study Case
### 3 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:**
- **First line of defence:** Setting strategy, performance measurement, and establishing and maintaining risk management, control, and governance across the business.
- **Second line of defence:** Providing a risk framework to improve decision making, planning, and prioritisation of the business activities.
- **Third line of defence:** Provides independent and objective assurance of the overall adequacy and effectiveness of governance, risk management, and controls within the business.

---

**Assurance Providers:**
- **First line of defence:** Management, Quality assurance functions, Other: Project Management Office
- **Second line of defence:** Assurance Providers: Risk: Risk Management, Regulatory Risk Management, Legal Risk Management, Other: Forensics, Consultancies within the business, e.g. Tax.
- **Third line of defence:** Assurance Providers: Internal Audit, External Audit/Advisors, External regulators

---

**Questions:**
- Is there any silo approaches and/or competing one another?
- Is any potential redundancy and/or assurance fatigue within assurance clients?
- Are they competent enough?
- Are these effective enough?
Assurance Providers

There are three fundamental classes of assurance providers:

1. **Those who report to management** 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.
3. **Those who report to external stakeholders** (financial statement assurance), a role traditionally fulfilled by the independent/statutory auditor.

Source: The Institute of Internal Auditors (IIA)
Why Combined Assurance?

- Optimize the **effectiveness of assurance providers**, create a synergy between assurance providers and avoid assurance fatigue.

- To improve coverage of the wider audit universe through combined assurance.

- To create confidence in the assurance has been provided on key/significant risks and to promote efficiency.

- To implement *Standard 2050* of IPPF & King III (South Africa).

What is the **difference** between Combined Assurance & Integrated Assurance?
Combined Assurance Approaches

• Combined assurance integrates & co-ordinates all assurance, by:
  1. Understanding the risks. Aligning assurance to the critical risk exposures;
  2. Understanding who are all the assurance providers;
  3. Realization of what is actually assurance;
  4. Reported within the governance structures;
  5. Coordinating the assurance activities; and
  6. Consolidating the risk and assurance profile.

• Two approaches:
  1. Top-Down
  2. Bottom-up

Source: PwC Combined Assurance Practical Approach
Combined Assurance Approaches – Top Down

- Assess Assurance Received
- Assess Assurance Providers
- Organisation Strategic Risks per Risk System
- Identify Risk Owners
- Identify Control Strategies
- Identify Assurance Providers

Source: PwC Combined Assurance Practical Approach
Combined Assurance Approaches – Bottom Up

• Reviews by “offsite” subject matter experts to be conducted during these time windows
• Reviews to be coordinated by Internal Audit
• An experienced leader appointed to manage each departmental review
• Reviews cover system compliance and effectiveness and opportunities
• Review findings are prioritised and ranked
• Review findings are referenced back to the risk register

Source: PwC Combined Assurance Practical Approach
2050 – 1 Coordination
Organization’s assurance provider framework can consist of internal audit, external audit, governance, risk management, or other business control functions.

2050 – 2 Assurance Maps
Assurance map is a valuable tool for coordinating risk management and assurance activities.

2050 – 3 Reliance on the Work of Other Assurance Providers
The results of other assurance providers can be integrated with the work of internal audit in a comprehensive opinion to key stakeholders. A good coordination attracts greater reliance on internal audit.

Internal Audit as Catalyst of Combined Assurance
bringing new perspective in Governance, Risk & Control and promote Combined Assurance through establishment of CAR Forum.

Combined assurance should be based on identified risks and how assurance is achieved and reported to the Board / Accounting Authority.
What are the Critical Success Factors of Combined Assurance?

1. Establish the Coordination among the Assurance Providers

2. Integrated Risk & Control Identification, Measurement & Reporting

3. Continuous Improvement of Risk & Assurance Maturity
Standards 2050 - Coordination

- The Chief Audit Executive should share information and coordinate activities with other internal and external providers of assurance and consulting services to ensure proper coverage and minimize duplication of efforts.
- This responsibility requires the CAE’s inclusion and participation in the organization’s assurance provider framework. This framework can consist of internal audit, external audit, governance, risk management, or other business control functions/disclosures performed by the organization’s management team.
- Inclusion and participation in this framework helps ensure that the CAE is aware of the organization’s risks and controls in relation to organizational goals and objectives.
- Boards will use various sources to gain reliable assurance, including management, internal audit, and third parties.

Source: The Institute of Internal Auditors (IIA)
Practice Advisory 2050 – 1 Coordination

• Oversight of the work of external auditors, including coordination with the internal audit activity is the responsibility of The Board
• Coordination of internal and external audit work is the responsibility of The Chief Audit Executive
• The CAE obtains the support of the board to coordinate audit work effectively.
• The external auditors may rely on the work of the Internal Audit Activity in performing their work.
• Planned audit activities of internal and external auditors need to be discussed to ensure that audit coverage is coordinated and duplicate efforts are minimized where possible.
• These assist external auditors in determining and adjusting the scope and timing of their work.
• On the other hand, external auditors presentation materials and management letters need to be understood by the CAE and used as input to internal auditors in planning the areas to emphasize in future internal audit work.

Source: The Institute of Internal Auditors (IIA)
Practice Advisory 2050 – 2 Assurance Maps

- Increased focus on the roles and responsibilities of senior management and the Board has prompted many organizations to place a greater emphasis on assurance activities.

- This guidance addresses how the Board is responsible for ensuring that business-critical risks are being assured and adequately managed.

- An “assurance map” is an organizational tool that will prevent redundancy, as well as some areas falling through the cracks.

Source: The Institute of Internal Auditors (IIA)
Practice Advisory 2050 – 2 Assurance Maps

• The Standards defines Assurance as “an objective examination of evidence for the purpose of providing an independent assessment on governance, risk management, and control (GRC).

• Assurance Map provides:
  • Who is doing what,
  • What has been done to date,
  • Provides comfort to those at the top that all participant are being responsible and accountable

• Steps of creating Assurance Mapping:
  • 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

Source: The Institute of Internal Auditors (IIA)
Assurance Reality Check

• Identify Assurance Provider (Internal Audit, Risk Management, Compliance, Information Security, SOX Compliance, Quality Assurance)

• Competency Assessment of Assurance Provider:
  • Skill & Experience levels
  • Scope & frequency of work
  • Acceptable approach/methodology
  • Conflict of Interest
  • Number of staffs
  • Quality review
Risk Mapping with ERM Fundamentals

• Risk naming conventions
• Shared understanding of risk and control information
• Proper risk description
• Agreement on residual risk exposure and target (desired) risk rating
• Understanding if controls really mitigate risk exposure
• Does the information on incidents feed back to the risk register
## Sample of Risk Mapping

<table>
<thead>
<tr>
<th>Example IT risk</th>
<th>Associated controls</th>
<th>Three lines of defence assurance providers</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>First line of defence - Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Second line of defence – Risk and legal based assurance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Third line of defence – Independent assurance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Control self assess</td>
</tr>
</tbody>
</table>

### Operational - Network

<table>
<thead>
<tr>
<th>Security breach</th>
<th>Secure firewall configuration</th>
<th>Secure remote access design</th>
<th>Security monitoring service contracted with supplier</th>
<th>Service level agreement with supplier</th>
<th>Disaster recovery plan</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Currently providing assurance</td>
<td>Should provide assurance</td>
<td>Quality of assurance acceptable</td>
<td>Quality of assurance unacceptable</td>
<td></td>
</tr>
</tbody>
</table>

Scope excludes detailed configuration
Sample of Assurance Mapping & Reporting

<table>
<thead>
<tr>
<th>Processes</th>
<th>Three lines of defence assurance providers</th>
<th>First line of defence - Management</th>
<th>Second line of defence – Risk and legal based assurance</th>
<th>Third line of defence – Independent assurance</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Control self assess</td>
<td>Mgt review</td>
<td>Special project</td>
<td>ERM</td>
</tr>
<tr>
<td>Strategic</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Funding</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sustainability</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Growth</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operational</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Treasury</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Products and services</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Finance</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Extensive assurance
- Moderate assurance
- Inadequate assurance
- Not applicable

Source: IIA Conference 2012: Risking It Combining It, Jhetam, Bilal
Sample of Assurance Mapping & Reporting

### Example of ranking of assurance

<table>
<thead>
<tr>
<th>Rating</th>
<th>Description/Characteristics guidance</th>
</tr>
</thead>
</table>
| Extensive Assurance     | • Scope of work covers entire process area  
                          • Period of the work performed covers more than half the year  
                          • Positive opinion or certification is provided  
                          • Accredited assurance provider |
| Moderate Assurance       | • Scope of work covers part of the business process  
                          • Work performed covers less than 6 months of the period under review  
                          • Limited assurance statement provided |
| Limited Assurance        | • Scope of work covers a very specific part of the business process  
                          • Work performed is for a period less than 3 months or is at a point in time  
                          • No certification or assurance statement provided (e.g. factual findings with recommendations) |

Source: IIA Conference 2012: Risking It Combining It, Jhetam, Bilal
Sample of Assurance Mapping & Reporting

<table>
<thead>
<tr>
<th>Risk No</th>
<th>Risks</th>
<th>Control Self Assessment</th>
<th>Management Review</th>
<th>IRM</th>
<th>Compliance &amp; Regulatory</th>
<th>Legal</th>
<th>Internal Audit</th>
<th>External Audit/Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ABC is unable to control minimise reputational damage during crises and unable to restore reputation due to non approval of communication strategies</td>
<td>Not applicable</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Uninformed, de-motivated workforce caused by lack of relevant and timely communication</td>
<td>Not applicable</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Not meeting the milestones for new organisational design</td>
<td>Not applicable</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Equipment theft &amp; vandalism</td>
<td>Not applicable</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Energy theft</td>
<td>Not applicable</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Inability to collect all our revenue</td>
<td>Not applicable</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Inadequate Engineering Definition During Project Planning and Development</td>
<td>Not applicable</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Delays in Acquiring Servitudes</td>
<td>Not applicable</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Investment decision delays</td>
<td>Not applicable</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Primary Energy Challenges</td>
<td>Not applicable</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Shareholder support</td>
<td>Not applicable</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Loan - Inadequate revenue to service Investec Loan</td>
<td>Not applicable</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: PwC Combined Assurance Practical Approach
Sample of Assurance Mapping & Reporting (cont’d)

Source: PwC Combined Assurance Practical Approach
### Sample of Assurance Mapping & Reporting (cont’d)

<table>
<thead>
<tr>
<th>Ref No</th>
<th>Risk description</th>
<th>Mitigating actions (existing or planned)</th>
<th>Accountable</th>
<th>Responsible</th>
<th>Assurance Provider</th>
<th>Nature of Assurance</th>
<th>To whom reported</th>
<th>Management Assessment</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Legislation and regulatory changes and uncertainty threaten the sustainability of ABC</td>
<td>Maintain marketing position of quality fuels: Increase availability on the forecourts.</td>
<td>GM: Sales &amp; Marketing</td>
<td>Legal &amp; Compliance officer</td>
<td>Line 1: Manager</td>
<td>Line 1: Monitor sales on a monthly basis (Niec product sales vs. Lead replacement product sales) with a report.</td>
<td>Line 1: GM level &amp; Mancom</td>
<td>Room for improvement</td>
<td>Infrastructure not available.</td>
</tr>
</tbody>
</table>
Practice Advisory 2050 – 3  Reliance on the Work of Other Assurance Providers

Five Principles in Determining Reliance:

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

Source: IPPF of IIA, Practice Guide Reliance by Internal Audit on Other Assurance Providers, Dec 2011
Assurance Maturity Model

Internal Audit Roles in Combined Assurance

- IA assisted in coordinating the initial development of consolidated risk assurance maps
- Together with Risk Management, IA coordinated with Business and Support units in validating the consolidated assurance maps
- Review the application and effectiveness of Combined Assurance practice:
  - Assess the quality of assurance
  - Assessment of the adequacy of Combined Reporting (combined assurance reporting)

**Risk Maturity : At which Risk Maturity Level ?**

**Partnership concept**

<table>
<thead>
<tr>
<th>Risk Maturity</th>
<th>Key Characteristics</th>
<th>Internal Audit Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Traditional</strong></td>
<td>No formal approach developed for risk management</td>
<td>Promote risk management and rely on audit risk assessment</td>
</tr>
<tr>
<td><strong>Awareness</strong></td>
<td>Scattered silo based approach to risk management</td>
<td>Promote enterprise-wide approach to risk mgt and rely on audit risk assessment</td>
</tr>
<tr>
<td><strong>Defined</strong></td>
<td>Strategy and policies in place and communicated. Risk appetite defined.</td>
<td>Facilitate risk management/liaise with risk management and use management assessment of risk where appropriate.</td>
</tr>
<tr>
<td><strong>Managed</strong></td>
<td>Enterprise wide approach to risk management developed and communicated.</td>
<td>Audit risk management processes and use management assessment of risk as appropriate.</td>
</tr>
<tr>
<td><strong>Integrated</strong></td>
<td>Risk management and internal control fully embedded into the operations.</td>
<td>Audit risk management processes and use management assessment of risk as appropriate.</td>
</tr>
</tbody>
</table>

Source: The Institute of Internal Auditors
Combined Assurance
“CIMB Niaga Case Study”

ASEAN FOR YOU
The Black Hole of Assurance

• The economic crisis provides evidence that boards of directors operate in a partial assurance vacuum, whereby boards rely on their top executive teams to provide the assurance, but too often that assurance is partial and insufficiently objective.

• Filling the board’s assurance vacuum (black hole) will require a change in internal auditing paradigm, positioning, and reporting method.

• Future CAEs, while remaining independent of the board, will need to have equal status with executive directors so that they can interface on equal terms and attend board meetings as well as some board committee meetings.

CIMB Niaga Chief Audit Executive is part of Board of Management, and actively being involved in several High Level Committee with regards to Governance, Risk, Compliance

Repositioning internal audit functions within their respective organizations will help provide stronger assurance to the board.

Source: Chambers, Andrew., The Black Hole of Assurance, IIA Governance Perspective, 2009
 Coordination of Compliance, Audit & Risk Management

- **Risk Monitoring Committee**
  - Define Risk Management Framework & policy
  - Enterprise wide risk identification and risk management

- **Risk Management**

- **Compliance**
  - Ensure compliance at all levels
  - Maintain pre-emptive and preventive controls

- **Business Unit/Management**
  - Identify key business risks
  - Update risk profile data

- **Quality Assurance**
  - Check implementation of control
  - On time & preventive control checks

- **Internal Audit**
  - Risk based audit
  - Strategic business partner
  - Detect, control & check

- **Audit Committee**
Make Combined Assurance a Reality

• Executive sponsor, audit committee support and management commitment
• Combined Assurance Champion, driving day-to-day activities:
  • Needs to be driven actively
  • Consistent reporting structure and feedback
  • Regular assessment of quality of delivery
• Combined Assurance Forum (3 – 6 monthly assessment)
• Common Risk Language and Alignment
• Convince all stakeholders of future approach, create combined assurance blue print (assurance and risk mapping, combined assurance reporting and continuous improvement)
• Centralized libraries to ensure consistency and data integrity

Internal Audit can lead this process!
Milestones & Achievements

**Done**

- Established Compliance-Audit-Risk (CAR) Forum:
  - Local Compliance-Audit-Risk Forum – Monthly
  - Regional Compliance-Audit-Risk Forum – Annually
- Role sharing between assurance providers has been discussed and formulated with regards to significant products & activities (facilitated by Group Internal Audit and Group Risk Management)

**Strategic Initiatives**

- Work in progress (could be facilitated by Internal Audit):
  - Formal Assurance Mapping between assurance providers
  - Centralized Risk & Control Library across the assurance providers
Aligned & Centralized Risk-Control Database across Assurance Providers

Risk Management Process

Process Owner (Working Unit)
- Risk Strategy
- Risk Maturity
- Risk Assessment
- Risk Awareness & Ownership (Risk Culture)

Risk Management Unit
- Risk Control Matrix
- Risk Profiling & Reporting
- Risk Methodology & Enforcement

Internal Audit Unit
- Evaluate Risk Management Process
- Risk Based Control Auditing
- Risk Based Audit Planning

Risk Based Audit Plan
Risk Based Audit Planning
Risk Culture
Thank You