Combined assurance
Integrating the role players to paint the full picture

Public Sector Risk Management Forum
7 March 2013
Contents

Defining combined assurance
Key objectives of a combined assurance framework
Sources of assurance
The governance model
Written assessment by Internal Audit
Aligning the role players
An approach to developing a combined assurance model
Reporting – completing the pyramid
Market trends
Answering the questions posed…
Combined assurance per the standard...

King III defines Combined assurance as follows:

Integrating and aligning assurance processes in a company to maximise risk and governance oversight and control efficiencies, and optimise overall assurance to the audit and risk committee, considering the company’s risk appetite.

Role of the audit committee:

The audit committee should ensure that a combined assurance model is applied to provide a coordinated approach to all assurance activities

The audit committee should ensure that the combined assurance is received is appropriate to address all the significant risks facing the company.

The relationship between the external assurance providers and the company should be monitored by the audit committee.

Role of Internal Audit:

King recommends that Internal audit should form an integral part of the combined assurance model as internal assurance provider.
Defining combined assurance

Integrating **assurance processes** in a company to:
- maximise risk and governance oversight and control efficiencies, and
- optimise overall assurance to the audit and risk committee,
- considering the company's risk appetite

Nothing more than formalising the process to assess and provide assurance over the adequacy and effectiveness of the control environment to manage risks resulting from the overall business strategy

**OR**

A co-ordinated approach that ensures that all assurance activities provided by management, internal assurance providers and external assurance providers adequately address significant risks facing the company and that suitable controls exist to mitigate these risks.
Key objectives of a combined assurance framework

Optomise assurance coverage
Coordinating the efforts of management, internal and external assurance providers

Systematic assessment of key risks associated with strategic objectives
Extent to which risks have been fully identified and responded to, based on an organisation's strategic objectives

Support the audit committee in assessing the effectiveness of internal financial control
Assurance to the board of directors in making their statements on internal control in the integrated report

Provide context of the impact of inadequate and ineffective control
Quantitative and qualitative impact of control breakdowns on the overall control environment

And ultimately, to fulfil the Audit Committee’s responsibility to monitor the appropriateness of the combined assurance model and its effectiveness in ensuring the significant risks are adequately addressed
Sources of assurance

- Strategy
- Operations
- Finance & Treasury
- Information Technology
- Human Resources
- Product development
- Sales
- Supply chain / Distribution
- Production
- Other

Management assurance

- Risk management
- Regulatory Compliance
- Internal Audit
- Legal
- Company secretary
- Health and Safety
- Other)

Internal assurance

- External audit
- ISO
- NOSA
- Sustainability
- Actuarial
- Project management
- Process improvement
- Other

External assurance
The governance model

Governance

Board and Committees
- Charters
- Structure / composition
- Ethics / Conduct
- Reporting

Operating framework
- Operating model
- Committees
- Delegated Authority
- Policies

Risk management
- Framework
- Tools
- Culture
- Response
- Monitoring
- Reporting
- Strategic risk
- Financial risks
- Technology / Data risk
- Project risk
- Reputational risk
- Regulatory / Legal risks
- Fraud risk
- Tax risk
- Sustainability risk
- People risk
- Operational risk

Risk mitigation strategies

Control framework
- Program management
- Financial
- Operational
- IT infrastructure
- Legal & regulatory compliance
- IT applications & data management

Assurance

Risk aligned, integrated, efficient, effective, sustainable
The governance model

**Board**
- Custodian of corporate governance
- Strategy / Risk / Performance / Sustainability oversight
- Delegation of key functions to structured committees
- Framework for delegation of authorities
- Group vs. subsidiary framework

**Audit**
- Financial risk, reporting and control (incl related fraud and IT risks)
- Integrated reporting oversight
- Internal and External Audit relationship
- Combined assurance

**Risk**
- Governance of risk
- Risk appetite and tolerance
- Oversight of establishment of the risk management framework
- Ongoing oversight over risk identification, response, monitoring, reporting and overall risk management

**Other**
- Nominations
- Remuneration
- Social & Ethics
- Governance
- Sustainability
- IT Steering

**Company secretary**
- Guidance to Board and individual directors
- Director induction, orientation and ongoing training
- Update of charters and terms of reference
- Papers, agenda, minutes

---

**Oversight**

**Strategy**
- Finance
- Human resources
- Information services
- Human Resources

**Management**

- Finance
- Human resources
- Information services
- Human Resources

**Enterprise risk management**
- Owner of risk framework
- Aligned framework incorporating key risk areas
- Risk infrastructure
- Risk policy and methodologies

**Compliance**
- Support management in ensuring compliance with laws, codes and standards
- Identify regulatory universe
- Develop risk management plans
- Monitor compliance

**Forensics**
- Support management in identifying fraud risks
- Establish fraud risk management framework and processes
- Monitoring and reporting
- Investigation

**Legal**
- Support management in identifying legal risk
- Establish frameworks and processes to manage legal risk
- Contract compliance
- Advice, Investigation, Litigation support

**Health and safety**
- Support management in managing health and safety
- Establish frameworks and responsible individuals
- Monitoring and reporting

**Assurance**

- Independent assurance over the control environment
- Risk based approach driven by risk identified across the organisation

**Internal Audit**
- Independent assurance over statutory financial reporting

**External Audit**
- Independent assurance over statutory financial reporting

---

8 Combined Assurance
Three lines of defence

1st line of defence – management assurance
- Assists in setting and executing strategies.
- Provides direction, guidance and oversight.
- Promote a strong risk culture & sustainable risk return thinking.
- Promote a strong culture of adhering to limits and managing exposure.
- Ongoing monitoring and management of risks.

2nd line of defence – Risk Management
- Formal, robust and effective risk management within which the organisations policies and minimum standards set.
- Objective oversight and ongoing challenging of risk management and performance while reporting is achieved across the business units.
- Overarching risk oversight across all risk types.

3rd line of defence – Internal Audit & other independent assurance providers
- Independent and objective assurance of overall adequacy and effectiveness of governance, risk management and control within organisation as established by 1st and 2nd line of defence.
- Ability to link business and risk with process and IT know how.
Written assessment by Internal Audit
The requirement

Internal Audit should provide a written assessment of the **effectiveness** of the company's system of **internal control** and **risk management** (to the Board through the Audit Committee):

- Internal Financial Control Assessment
- Overall assessment of the control environment
- Assessment on the Risk Management processes and procedures

- Not limited to financial control (strategic, financial, operational, compliance, sustainability)
- Strong reliance on risk management
- Assessment of design, implementation and effectiveness of control
- Within a defined materiality (coverage & level of assurance)
- Assessment of the impact of weaknesses in financial control (financial loss, fraud, material error)
- External audit as an external assurance provider
# Written assessment by Internal Audit

**Level of assurance (IIA Standards 2010.A2/2450)**

<table>
<thead>
<tr>
<th>Audit universe</th>
<th>What is in and out of scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>Materiality framework</td>
<td>Extent of testing / Level of risk</td>
</tr>
<tr>
<td>Timing and frequency of testing</td>
<td>Assessment of operating effectiveness throughout the period under review</td>
</tr>
<tr>
<td>Audit evidence</td>
<td>Overall adequacy and appropriateness to support conclusions reached</td>
</tr>
<tr>
<td>Results of testing</td>
<td>Individual and overall impact of control deficiencies</td>
</tr>
</tbody>
</table>

**Negative vs. Positive assurance**
Aligning role players

Organisation Strategy

Strategic Objectives

Risks circumventing achievement of Strategic Objectives

Internal Controls

Combined Assurance

Written Assessment by Internal Audit

Combined Assurance

Management

Compliance

Risk Management

Tax

Operational

Legal

Compliance

Strategic

Risk Appetite

Bottom Up

Financial

Internal Audit

External Audit

Governance

Statutory Actuary

Written Assessment by Internal Audit

By Internal Audit

Organisation Strategy

Strategic Objectives

Risks circumventing achievement of Strategic Objectives

Internal Controls

Combined Assurance

Written Assessment by Internal Audit

By Internal Audit

Organisation Strategy
Example of a combined assurance model
### An approach to developing a Combined Assurance framework

<table>
<thead>
<tr>
<th>Align framework</th>
<th>Identify risks</th>
<th>Document controls</th>
<th>Design &amp; Implementation</th>
<th>Plan assurance</th>
<th>Aggregate results</th>
<th>Report</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assess the governance model and identify the assurance providers across the group</td>
<td>Risk identification and mapping</td>
<td>Assess the overall internal controls framework and identification of controls to mitigate risks</td>
<td>Initial assessment of design, implementation and effectiveness of entity level controls on a top down basis to confirm completeness of the control framework and identify key gap and remEDIATE</td>
<td>Develop combined assurance plan</td>
<td>Compile reporting to enable overall written assessment by Internal Audit</td>
<td>Compilation of report, and validation of level of assurance provided to the Audit Committee based on scope of assurance, results and other qualitative considerations</td>
</tr>
<tr>
<td>Align governance model</td>
<td>Initial understanding of the maturity of the risk identification framework (role played by risk management)</td>
<td>Identify entity level controls</td>
<td>Document processes and controls</td>
<td>Specific assurance by assurance provider</td>
<td>Align reporting, rating and escalation framework</td>
<td>Management self assessment</td>
</tr>
<tr>
<td>Align specific mandate, roles and responsibilities of assurance providers</td>
<td>Validation of existing risk map and confirmation of key risks across the organisation (workshops, detailed mapping etc)</td>
<td>Identify key controls across all key operations and functions across the organisation</td>
<td>Identify control gaps</td>
<td>Matrix against key risks and controls identified across the organisation</td>
<td>Ongoing assessment of assurance achieved against planned, and impact on overall assurance</td>
<td>Ongoing monitoring and assurance from Risk and related assurance providers</td>
</tr>
<tr>
<td>Define common risk, control and reporting framework</td>
<td>Group level key risk identification</td>
<td></td>
<td>Develop remediation plans and actions</td>
<td>Define level of control and assurance for each assurance provider</td>
<td>Aggregation of results of assurance activities and causal analysis of potential impact of findings</td>
<td>Independent internal assurance from Internal Audit</td>
</tr>
<tr>
<td>Technology enablers to support common risk and control framework, and report on ongoing assurance</td>
<td>Business unit and support function key risk identification</td>
<td></td>
<td></td>
<td>Ongoing alignment and project management of the combined assurance framework and plan Combined assurance (PMO), including change management and awareness</td>
<td>Consideration of control and issue trends and themes</td>
<td>Independent external assurance from External Audit and other external assurance providers</td>
</tr>
<tr>
<td>Integrate control requirements and rationalise controls</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Strategic objective
- Identify & document process
- Identify key risks
- Identify key controls
- Assess design & implementation
- Test control effectiveness
- Evaluate results
<table>
<thead>
<tr>
<th>Assurance Provider</th>
<th>Management</th>
<th>Management</th>
<th>Internal Audit</th>
<th>External Audit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Info Source</td>
<td>Group Strategic Risk Register</td>
<td>IFC Framework</td>
<td>Internal Audit Reports</td>
<td>Annual Reports - AFS</td>
</tr>
<tr>
<td>Workings</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Appendix</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Technology Risk Intelligence Map**

- **Governance**
- **Strategy and Planning**
- **Infrastructure**
- **Innovation & Growth**
- **Operations**
- **Compliance**
- **Reporting**

- **Mix Telematics Management risks**
- **Mix Telematics management risk assurance**
- **Mix Telematics Internal Audit Assurance**
- **Mix Telematics External Audit Assurance**

© 2011 Deloitte
Types of controls

- **Company Level Controls**
  - Control Environment
  - Risk Assessment
  - Information & Communication
  - Monitoring

- **Entity Level Controls**

- **Process Level Controls**
  - Control Activities (Financial Reporting & Closing, Treasury etc)

- **General Computer Controls**
  - Control Activities (Procurement, Inventory, Revenue etc)
## Illustrative combined assurance matrix

<table>
<thead>
<tr>
<th>Processes</th>
<th>Three Types of Assurance Providers</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Management-based Assurance (First Line of Defence)</td>
</tr>
<tr>
<td></td>
<td>Management Reviews</td>
</tr>
<tr>
<td></td>
<td>Risk Management</td>
</tr>
<tr>
<td><strong>Strategic</strong></td>
<td></td>
</tr>
<tr>
<td>Sustainability</td>
<td>✔</td>
</tr>
<tr>
<td>Growth / Mergers &amp; Acquisitions</td>
<td>✔</td>
</tr>
<tr>
<td>Funding</td>
<td>✔</td>
</tr>
<tr>
<td><strong>Operational</strong></td>
<td></td>
</tr>
<tr>
<td>Financial</td>
<td>✔</td>
</tr>
<tr>
<td>Treasury</td>
<td>✔</td>
</tr>
<tr>
<td>Human Resources</td>
<td>✔</td>
</tr>
<tr>
<td>Information Technology</td>
<td>✔</td>
</tr>
<tr>
<td>Supply Chain</td>
<td>✔</td>
</tr>
<tr>
<td>Environment</td>
<td>✔</td>
</tr>
<tr>
<td>Quality</td>
<td>✔</td>
</tr>
<tr>
<td>Products and Services</td>
<td>✔</td>
</tr>
<tr>
<td>Customers</td>
<td>✔</td>
</tr>
<tr>
<td>Compliance</td>
<td>✔</td>
</tr>
<tr>
<td>Reporting: Financial &amp; Sustainability</td>
<td>✔</td>
</tr>
</tbody>
</table>
Questions to ponder? – achieving the goal

• Develop a combined assurance framework
• Align the existing governance model to leading practice
• Assess the effectiveness of the risk management framework and processes and enhance risk governance, infrastructure and ownership (risk governance, risk framework and methodologies, risk appetite and tolerance, risk assessments, risk mitigation and control remediation)
• Assess the overall effectiveness of internal assurance providers including Internal Audit, Regulatory compliance, and Risk management (role and remit, position, people, processes, and performance)
• Identify key risks across the business
• Integrating and aligning the Internal controls framework in an organisation
• Assess the design, implementation and effectiveness of entity level controls
• Document processes and assess the design and implementation of key controls
• Test the effectiveness of key controls
• Develop the overall assurance and related materiality framework and approach for Internal Audit in supporting it’s overall level of assurance to the Audit Committee
• Support Internal Audit in assessing the level of assurance in its written assessment to the Audit Committee
Completing the pyramid

Risk Reporting

Internal Audit Reporting

Management Reporting pertaining to risks and opportunities (e.g. SHEQ, KPIs, KRIIs)
Completing the pyramid

Information presented to Board & Executives

Data is refined and reduced to information

Risk Management Reporting

Internal Audit Reporting

Management Reporting pertaining to risks and opportunities (e.g. SHEQ, KPIs, KPIs)
Trends we see in the market – strengths to build on

1. **A combined assurance approach is mostly already in place** – to an extent – which is a good starting point. The approach typically requires some further tweaking and embedding into the day to day business activities.

2. **A three lines of defence assurance model is typically already established**, where the first, second and third line assurance providers are already involved in the business with their roles being fairly mature (except perhaps for the management self-assessments).

3. **An ERM framework is mostly already in place.** This integrates the business objectives with business processes and key risks.

4. **A Financial control framework and IT governance** is often already in place, however not tied into the ERM and expanded to also cover non-financial controls, and not necessarily integrated.
Trends we see in the market – for improvement

1. Enhancing transparency in terms of overall (combined) assurance results (data vs information for decision making)

2. The combined assurance scope mainly covering financial risks, should cover all material risks.

3. Structuring of the combined assurance team, oversight.

4. Overall combined assurance framework not always in place or not integrated.

5. Management Self Assessments (MSA’s) not always in place - this may be an efficient way of bedding accountability down and establishing a stronger risk / control culture.
Linking combined assurance and institutional performance

- Golden thread between strategy, risk, control and performance
- Risk control – relationship
  - What are the risks to and of the strategy?
  - How do we control those risks?
  - Effective risk management = a better chance of achieving strategy
  - Achieving strategy = performance
- Providing the evidence for performance – not just 1 measure of success
The impact on risk

- Aligning strategy and risk management
  - Not just a once a year strategic workshop
  - Unpacking and understanding what the strategy means
  - On-going monitoring of red flags
- Integrating risk with other role players
  - Audit
  - Broader risk players – compliance, forensics, IT
- Communication
  - Combined assurance forum
  - With management
- Reporting
  - Demonstrating the golden thread
  - Integrating reporting
Strengthening cross cutting organisational controls

• Defining control
  • A control is merely a response to managing risk
  • Controls are often based on past experience and embedded in individuals
  • Policies, procedures and guidelines are the collection of controls
  • Controls evolve
• Are organisations being intentional about control?
  • Control framework design
  • Regular review of core processes for adequacy, effectiveness, efficiency and quality
  • Is there a demonstrable link between risk and control?
• Cross cutting versus functional processes and controls
  • Is risk being leveraged to assess organization wide response to specific risks? – e.g. fraud risk
  • Consideration of the governance model in assessing controls
  • Are you able to provide assurance over organisation wide risks?
CONTACT DETAILS

For more details contact

Mark Victor
Director: Risk Advisory
082 772 3003
(011) 806 5594
mvictor@deloitte.co.za