Combined Assurance in today’s world of internal audit
With combined assurance, there will be a number of parties involved in providing assurance, and their activities require coordination and alignment.

Familiarity with Combined Assurance

• Globally, 59% of respondents were aware of combined assurance, although there were large differences between regions.

Implementation of Combined Assurance

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%).

What is combined assurance?

Combined assurance is defined as...

“integrating and aligning assurance processes in an organisation 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”.  *King III report*

“The alignment of governance, risk and assurance activities – linking them with company strategy and business model – to better co-ordinate efforts and reporting with the aim of improving business performance and resilience”
### What is combined assurance?

<table>
<thead>
<tr>
<th><strong>What it <em>is</em>...</strong></th>
<th><strong>What is it <em>NOT</em>...</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ Starts with understanding strategic objectives, mission and business model</td>
<td>▪ Just a new reporting approach</td>
</tr>
<tr>
<td>▪ Involves co-ordination of assurance efforts and reporting across various oversight functions (e.g., Group Finance, Treasury and Management Risk functions, Group Risk, Internal Audit, External Audit)</td>
<td>▪ Just a technology solution</td>
</tr>
<tr>
<td>▪ Encompasses people, processes and technology considerations</td>
<td>▪ An elimination of the need for existing assurance functions (e.g., Compliance/risk functions within Bus (e.g. Marketing trading risk management, Internal Audit, Group Risk))</td>
</tr>
<tr>
<td>▪ Promotes better leveraging of the “Three Lines of Defence” model</td>
<td>▪ An additional bureaucratic layer that adds additional paperwork/administrative input</td>
</tr>
<tr>
<td>▪ Converges risk, control and compliance data</td>
<td>▪ Just a conceptual framework – it must be practical</td>
</tr>
<tr>
<td>▪ Requires effective change management</td>
<td>▪ Achievable without buy-in from all key risk, control and compliance functions</td>
</tr>
</tbody>
</table>
What are we seeing?

BAC would like increased visibility into the links between strategy and risk, compliance and governance process. Regulations are managed independently resulting in a cumbersome, redundant, and expensive approach.

Control environments are still heavily manual despite all our investment in technology. They are not taking advantage of ERP functionality and automated controls.

Ineffective, scattered approach to risk, compliance and governance.

Whilst there is a Group level approach to risk assessment and reporting, risks & controls within organisation or within business units.

Looking for a solution that will bring down the amount of manual controls and increase automated controls.

Improve and rationalize information to drive business results.

Combined assurance.
What are we seeing (continued)

Boards of directors are tasked with securing stability and growth for shareholders in the challenging context of demonstrating sound governance and control, compliance with increasingly complex regulatory requirements, and proper engagement with and accountability to stakeholders.

They need to:
- Triangulate current strategy, risk, compliance, and performance
- Be forward looking, have access to horizon scanning of upcoming risks and challenges
- Establish risk appetite across all facets of risk (including compliance risks)
- Be assured and action focused
  - Risk escalation processes are in place and “work”
  - Actions identified to reduce risk are followed up and implemented
Uncoordinated: The impact on the business

COSO Review (annual review, facilitated by Group Finance)

Group Risk – Strategic and Operational Risk Management Process

Compliance monitoring activities performed by 1st line

Board has lack of clarity around current assurance activities across key business areas, risks and three lines of defence

Help!

Reporting from various first, second and third line assurance functions into various Executive and Board forums

Request for Internal Audit Testing Data

Periodic requests by Regulators
Uncoordinated: The impact on decision-making

Business Leaders largely rely on fragmented reporting that provides inadequate and untimely insights to make key business decisions. Common combined reporting challenges include:

- Lack of common language/taxonomy (e.g., risk rating scales)
- Disconnected reporting methodologies and calendars – more ad hoc than systematic reporting
- Silos – lack of data sharing between functions
- Use of incompatible reporting tools/technologies
- Business vs. compliance vs. audit view

<table>
<thead>
<tr>
<th></th>
<th>ERM</th>
<th>Audit</th>
<th>Compliance</th>
<th>SOX</th>
<th>Info Sec</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blue – 1</td>
<td>Insignificant</td>
<td></td>
<td>Process Improvement</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Green – 2</td>
<td>Minor</td>
<td>Low</td>
<td>Non-Reportable</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>Yellow – 3</td>
<td>Moderate</td>
<td>Medium</td>
<td>Reportable (to Division)</td>
<td>Control Deficiency</td>
<td>Medium</td>
</tr>
<tr>
<td>Orange – 4</td>
<td>Major</td>
<td>High</td>
<td>Reportable (to Executive)</td>
<td>Significant Deficiency</td>
<td>High</td>
</tr>
<tr>
<td>Red – 5</td>
<td>Critical</td>
<td></td>
<td>Reportable (to Board)</td>
<td>Material Weakness</td>
<td>Critical</td>
</tr>
</tbody>
</table>
Uncoordinated: The impact on assurance cost

Do you consider all the components that add up to the total cost of assurance? What impact can better combined assurance have on reducing the cost?

- **Corporate assurance**
  - Includes costs of monitoring all assurance providers

- **'Independent' assurance**
  - Includes costs of Internal Audit and other assurance providers

- **Ongoing assessment and monitoring**
  - Includes management’s time & costs in proving assurance

- **Business performance**
  - Includes opportunity costs lost where assurance effort ‘slow the business down’

**Total cost of assurance**
Drivers

A number of key enterprise challenges (some examples provided below) are compelling businesses to transform their various assurance functions – acting as key drivers to move towards integrated assurance that is leaner, safer and better.

Key enterprise challenges

- **Growth pressures**
  - Pressure to sustain growth & profitability increases risks related to product innovation, operating model transformations (i.e., shared services, use of technology, outsourcing etc.), and new markets
- **Risk content**
  - Board/Leadership is focusing on emerging risks and questioning completeness/quality of risk content
- **Talent management**
  - Increased risk of inadequate talent management due to pace of change, market conditions and organisational change
- **Right sizing**
  - Redundancy and/or overlap in risk management and assurance given lack of clarity in roles and responsibilities (convergence, single view of risk, assurance mapping)

Governance

- **Strategy**
  - Improved linkage to strategy
  - Better alignment to business
  - Competitive advantage

- **Performance**
  - Enhanced regulatory compliance
  - Reduction of costs
  - Improved risk intelligence
  - Greater transparency
  - Alignment through GRC tools

DRAFT
The evolving journey and maturity

1. Developing
   - Compliance focused
   - Limited visibility/brand
   - Limited use of data/technology
   - Developing relationships with the business

2. Mature
   - Actioning strategies outlined around controls self assessment, data analytics/continuous assurance/continuous monitoring, integrating assurance

3. Advanced
   - Collaborative business partner
   - Reputation as innovator
   - Extensive use of data analytics
   - Centre of excellence for Executives
   - Key agent of change
Main components to success

Shared integrated assurance vision and strategy

Three lines of defence/governance

Common language and shared methodology

Co-ordination of efforts and reporting

Change management
Main components to success (continued)

Shared combined assurance vision and strategy

In order to successfully implement a sustainable Combined Assurance program within an organisation, it should be strategically focused and aligned with the organisation’s mission, strategy, values and business model.

Key stakeholder involvement and buy-in to the combined Assurance vision and strategy is a critical factor for success. Without upfront alignment on the future-state vision, the program runs a high risk of failure.

Key steps:

- Define the overall vision, objectives and guiding principles for combined Assurance. When developing the vision/objectives, potential questions to consider include but are not limited to:
  - What does success look like? (e.g., alignment of x assurance processes, x% reduction of total cost of assurance)
  - What is the appropriate scope of the framework? (e.g., all assurance activities vs. selection)
  - What is the desired timing for achieving the stated vision?

- Identify all stakeholders
- Align expectations and understanding of mandate
- Perform inventory of current assurance practices and risk processes
- Identify future state reporting needs
- Define desired future-state and strategy to achieve it (e.g., project plan and detailed roadmap)
Main components to success (continued)

Key steps:

- Define oversight and monitoring responsibilities of the following roles:
  - Board oversight committee
  - Executive management
  - Management steering committee
- Assign the responsibilities for coordinating program implementation efforts to the appropriate person (e.g., CRO)
- Develop assurance map (e.g., by key risk)
- Develop a framework for assigning responsibilities across the three lines of defence
- At a key risk/process/account/system level using a matrix format, assign current-state roles and responsibilities
- Assess appropriateness and redirect resources where need to ensure that activities are focused on those areas with the greatest potential benefit for the business
- Develop and implement future-state design governance structure (long-term) and document the Combined Assurance operating structure with roles and responsibilities

Combined assurance promotes better leveraging of the “Three Lines of defence” model to give greater line of sight and clarity of accountability through the business for management and the Board.

Tools like assurance maps allow management and the Board to better see who is providing assurance on what, the main mitigation plans across businesses and any gaps that need to be addressed.

Three lines of defence/governance
Main components to success (continued)

Key steps:

- Standardize language and foundational elements across functions. This might include:
  - Definitions for key terms (e.g., risk, issue, mitigating activity)
  - Risk ranking criteria
  - Risk categories
  - Control types
  - Issue categories

- Refresh tools and templates to drive standardization across functions (e.g., update risk reporting dashboard with standardized language)

- Develop a methodology that provides a set of guidelines on the process to follow when performing key activities. For example:
  - How to identify key controls
  - Guidance on testing approach to use
  - Sampling guidance
  - Testing and documentation processes and templates
  - Guidance on interpreting the test results and reporting

Combined Assurance will not be possible without the harmonization of the language and methodology used.

Updated tools and templates can help enforce the use of common language and help guide process.

The use of common language and a shared methodology should be guiding principles when integrating assurance activities.
Main components to success (continued)

**Key steps:**

- Establish a Master Calendar Plan taking into account critical paths and minimum requirements. The Master Calendar Plan helps coordinate assurance function calendars to optimize and sequence activities and business touch points.
- Create a central repository for shared access to data and results.
- Perform a cross-functional coordinated risk assessment.
- Expand risk consideration into audit and compliance planning.
- Identify risk management gaps/duplication.
- Leverage all available testing resources for coordinated control testing.
- Enable process through technology.
- Continuous evaluation of the effectiveness of the process and tools being used.

**Co-ordination of efforts and reporting**

The scope, content and timing of the various activities across functions that perform them should be understood and strategically sequenced to help ensure information is shared and leveraged appropriately.

Consideration should be given to using the same technology solution or at a minimum creating a central repository or for sharing of data and results.
Change management

To transform to an enterprise-wide combined Assurance model, an organisation will need to take action to help its leaders, its people and stakeholders impacted by the changes move along the Commitment Curve to the desired future state whereby ultimately, they become advocates and owners of the new model.

Key steps:

- Perform a high level stakeholder & key influencer analysis
- Continuously identify and take action to align stakeholders on the overall Combined Assurance future state vision to move them up the Change Curve towards fully supporting the initiative. Activities might include:
  - Formal communication of the importance of and support for the program by Executive Management and relevant governance bodies
  - Formal education and awareness sessions for key stakeholders
  - A forum to allow input/feedback from stakeholders (e.g., suggestions to further enhance the program)
Example outcome illustration
Benefits to combined assurance for ABC Client

**Stakeholders**

- **CEO/Board**
  - Clear reporting linking strategy, risk, performance and controls

- **CFO**
  - Enhance Controls
  - Baseline controls operate effectively
  - Lower cost of business without increasing risk

- **Group Risk**
  - Enhanced oversight over cross-functional risk management activities and assurance

- **Group Executive Legal and Regulatory Affairs**
  - Integrated compliance at lower cost

- **Internal Audit**
  - Reduced costs and more “value add”

**Objectives**

- **CEO/Board**
  - Clear reporting linking strategy, risk, performance and controls

- **CFO**
  - Enhance Controls
  - Baseline controls operate effectively
  - Lower cost of business without increasing risk

- **Group Risk**
  - Enhanced oversight over cross-functional risk management activities and assurance

- **Group Executive Legal and Regulatory Affairs**
  - Integrated compliance at lower cost

- **Internal Audit**
  - Reduced costs and more “value add”

**Business case**

- Enhanced Insights
- Increased Stakeholder Confidence
- Enhanced control
- Reduced Cost
- Improved Risk Management

**Integrated assurance**
More transparency, less cost

Better understanding and management of the **total cost of assurance**

An **integrated** approach may have a high initial spend, but flattens over time **decreasing costs and improving efficiencies**!
## Example Assurance Map

<table>
<thead>
<tr>
<th>Business Type</th>
<th>Region</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corporate</td>
<td>North America</td>
</tr>
<tr>
<td>Shared service center</td>
<td></td>
</tr>
<tr>
<td>Paper</td>
<td></td>
</tr>
<tr>
<td>Industrial packaging</td>
<td></td>
</tr>
<tr>
<td>Pulp</td>
<td></td>
</tr>
<tr>
<td>Recycling</td>
<td></td>
</tr>
<tr>
<td>Finance</td>
<td></td>
</tr>
<tr>
<td>Business processes</td>
<td></td>
</tr>
<tr>
<td>Financial Reporting</td>
<td>C, D</td>
</tr>
<tr>
<td>Budgeting and Forecasting</td>
<td>C</td>
</tr>
<tr>
<td>Tax</td>
<td>C</td>
</tr>
<tr>
<td>Liquidity and Credit</td>
<td>C</td>
</tr>
<tr>
<td>Vendor Masterfile Maintenance</td>
<td>E</td>
</tr>
<tr>
<td>Vendor Selection</td>
<td>E</td>
</tr>
<tr>
<td>Payable Approval</td>
<td>E, C</td>
</tr>
<tr>
<td>Payable Processing</td>
<td>E, C</td>
</tr>
<tr>
<td>Accounts</td>
<td>E, C</td>
</tr>
<tr>
<td>Procure to Pay</td>
<td>E, C</td>
</tr>
<tr>
<td>Sales</td>
<td>E, C</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>E, C</td>
</tr>
<tr>
<td>Product Development</td>
<td>E, C</td>
</tr>
<tr>
<td>Operations</td>
<td></td>
</tr>
<tr>
<td>Sales</td>
<td>F</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>F</td>
</tr>
<tr>
<td>IT</td>
<td></td>
</tr>
<tr>
<td>Access Control</td>
<td>A, E</td>
</tr>
<tr>
<td>Asset Management</td>
<td>D</td>
</tr>
<tr>
<td>Change Management</td>
<td>A, E</td>
</tr>
<tr>
<td>IT</td>
<td></td>
</tr>
<tr>
<td>Compliance</td>
<td></td>
</tr>
<tr>
<td>Compliance (FCPA)</td>
<td>B, E</td>
</tr>
<tr>
<td>Corporate Governance</td>
<td>C, E</td>
</tr>
<tr>
<td>Legal</td>
<td></td>
</tr>
<tr>
<td>Regulatory</td>
<td>B</td>
</tr>
<tr>
<td>HR</td>
<td></td>
</tr>
<tr>
<td>Employee Masterfile Maintenance</td>
<td>C</td>
</tr>
<tr>
<td>Compensation and Benefits</td>
<td>E</td>
</tr>
<tr>
<td>Training</td>
<td>E</td>
</tr>
</tbody>
</table>

### Legend

- **Legend**
  - SSSE 16*: A
  - Health and Safety: F
  - Compliance (FCPA): B
  - Not Tested/Immaterial: C
  - SOX: D
  - 1st Line of defence: E
  - Business Continuity: F
  - 2nd Line of defence: E
  - Internal Audit: E
  - 3rd Line of defence: E
Example outcome - Three lines of defence

1st Line
- BU’s
- Divisions
- Risk & control identification
- Risk & control assessment
- Quantification & measurement
- Monitoring, testing, & verification
- Reporting

2nd Line
- ERM
- Compliance
- Privacy
- Information security
- QA/EHS
- SOX
- Internal audit

3rd Line
- Internal audit

Converged Activities
- Develop Enterprise Risk management Program
- Develop Compliance Program
- Develop Information Security Program
- Develop Audit/Compliance Programs
- Develop SOX Testing Plan
- Develop IA Plan

Discrete Activities
- Test controls periodically throughout the year
- Disseminate test results to respective risk and control groups
- Provide integrated guidance on risk assessment, quantification, and measurement
- Review and challenge current risk assessments performed within the business
- Coordinate calendars to perform additional procedures, as needed
- Identify controls to be tested

Stakeholders
- Independent testing
- Report on enterprise risk exposure
- Report on compliance with regulations
- Report on status of information security program and compliance
- Report on servicer compliance
- Report on financial reporting controls
- Provide assurance

* Note: This is not an exhaustive list of Business Units in the 1st Line of defence

- Flowchart process
- Identify risk and controls
- Link to SOX oversight
- Perform risk and control self assessments

- Identify KRI
- Capture risk loss data
- Perform scenario analyses
- Perform trend analyses

- Review and challenge current risk assessments performed within the business
- Coordinate calendars to perform additional procedures, as needed
- Identify controls to be tested

- Independent testing
- Report on enterprise risk exposure
- Report on compliance with regulations
- Report on status of information security program and compliance
- Report on servicer compliance
- Report on financial reporting controls
- Provide assurance
Change management commitment curve

- Unaware
  - I am unaware of the New Program

- Aware
  - I am aware of the New Program

- Understand
  - I understand the New Program and can explain it

- Acceptance
  - I accept the New Program (but don’t necessarily want it)
  - I do see the “benefits”

- Engagement
  - I am open to the New Program
  - I see how the New Program benefits me and the company
  - I am actively involved in making it happen!

- Advocacy & ownership
  - I support it
  - I believe in it
  - I recommend it
“When combining assurance, the role of internal audit is key in supporting the board in having effective oversight of the company. Otherwise, it does not work.” —Marie-Helene Laimay, CAE, Sanofi, France

<table>
<thead>
<tr>
<th>Lessons Learnt</th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ Internal audit has a key role to play in driving implementation</td>
</tr>
<tr>
<td>▪ Buy-in Support is required from the top</td>
</tr>
<tr>
<td>▪ Anticipated value should be articulated up front</td>
</tr>
<tr>
<td>▪ All participants should reach a consensus on taxonomy</td>
</tr>
<tr>
<td>▪ Control assessment and risk ratings should be standardised</td>
</tr>
<tr>
<td>▪ Level of maturity of the different players in the combined assurance field should be identified</td>
</tr>
</tbody>
</table>

- Implementing combined assurance is not something that can be achieved from one day to the next—it should be considered a journey.
## IIA Standards Related to Combined Assurance

<table>
<thead>
<tr>
<th>Standard</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard 1000: Purpose, Authority, and Responsibility</strong></td>
<td>The purpose, authority and responsibility of internal audit activity must be formally defined in an internal audit charter, consistent with the Definition of Internal Auditing, the Code of Ethics, and the standards</td>
</tr>
<tr>
<td><strong>Standard 2050: Coordination</strong></td>
<td>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 minimise duplication of efforts.</td>
</tr>
<tr>
<td><strong>Standard 2060: Reporting to Senior Management and the Board</strong></td>
<td>The Chief Audit Executive must report periodically to senior management and the Board. Reporting must also include significant risk exposures and control issues, including fraud risks, governance issues, and other matters needed or requested by senior management and the Board.</td>
</tr>
<tr>
<td><strong>Standard 2100: Nature of Work</strong></td>
<td>The internal audit activity must evaluate and contribute to the improvement of governance, risk management and control processes using a systematic and disciplined approach</td>
</tr>
</tbody>
</table>

- The *Standards* clearly supports the philosophy of combined assurance.
Questions
THANK YOU