www.pwc.co.za

Covering your bases

Implementing approriate levels of combined assurance

A framework for risk, control and assurance

pwc

Contents

Annexures

Combined assurance and corporate governance

Businesses are constantly being bombarded by new challenges, ever-increasing levels of complexity and, on top of that, market instability, each carrying its own risks. They are being forced to become more resilient to protect themselves against various volatile world events, regulatory changes and a host of enhancements to corporate governance. On top of that, stakeholder expectations are increasing, so that businesses have to cover themselves in that respect as well.

What all this boils down to is that businesses need to find a proper balance between safeguarding their operations and enabling strategic development and growth to gain shareholder and stakeholder confidence. Increased demands to protect stakeholder value necessitate that operational safeguards should be more proactive and forward looking. Boards have to start taking a broader and more holistic approach to risk and how they manage it. This will not only protect them, but also elevate them to become strategic drivers of performance rather than merely a reactive and compliance-driven function. It is a key task for boards to perform constant risk oversight, and more and more boards are starting to realise that risk cannot be managed only by specialist risk managers.

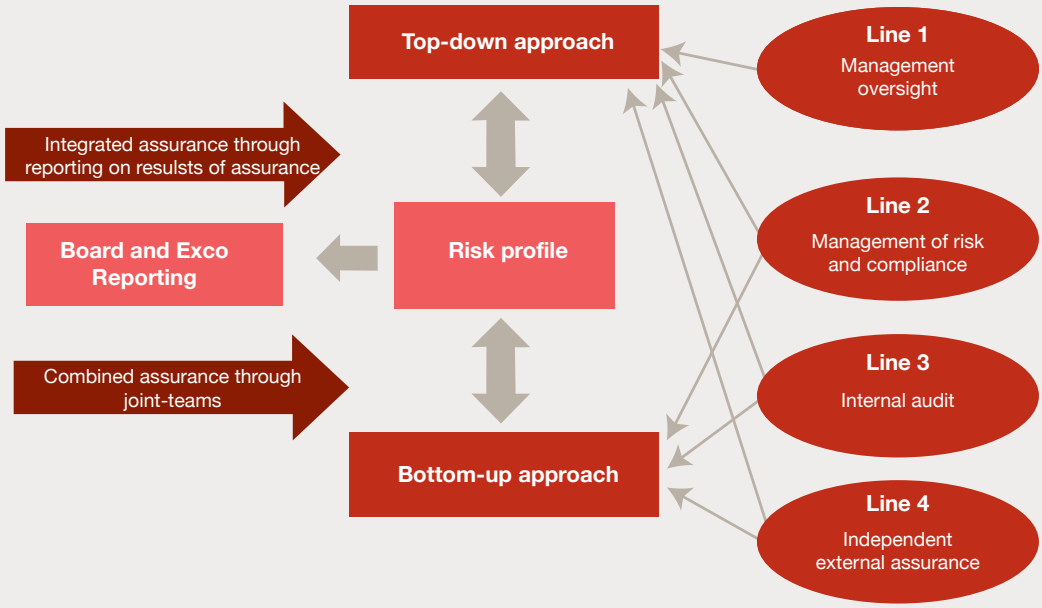
PwC has developed a risk assurance framework that includes a combined assurance model to help your business and its board explore where risk lies. This flexible and dynamic model encourages the board to adopt a broader perspective on risk and resilience and follow a future-facing approach in dealing with it by showing them how they can assess the impact of both known and unknown risk on company strategy. It is something that should form part of all board agendas to enable the board to uncover risks and opportunities that otherwise they would not have known existed.

The combined assurance model classifies the risk landscape into types of risk with a potentially positive or negative effect on the ability of your business to meets its strategy and protect or create value. It then goes on to formulate the approach to be followed in managing risk and the control and assurance continuum. In response to the question: What does your business have in place to protect itself? you need to assess four lines of defence. These lines of defence reside in the business's (1) people, systems and controls, (2) risk management and compliance function, (3) internal audit function and, finally, (4) independent external assurance.

Through the use of the combined assurance model, assurance gradually increases over the four lines, with the fourth line providing the highest and strongest level of assurance – taking independent assurance to the next level. We have designed the combined assurance model to achieve this gradually increasing level of assurance in our approach. This approach is explained in more detail on the next page.

The audit committee should ensure that a combined assurance model is applied to provide a co-ordinated approach to all assurance activities.

Process for integrating and co-ordingating assurance activities



Combined assurance should be based on identified risks and how assurance is achieved and reported to the board through the audit committee. It offers tangible benefits that extend well beyond proving compliance, including:

- Co-ordinated and relevant assurance efforts focusing on key risk exposures across the production life cycle;
- Minimised operational and business disruptions;
- Comprehensive and prioritised tracking of remedial action on identified improvement opportunities/weaknesses;
- Improved reporting to the board and committees, including reducing the repetition of reports for review by the different committees;
- Possible reduction in assurance costs;
- Optimised assurance spend in that auditors are assisted in giving opinions on residual risk status, prevention of assurance fatigue, minimised overlap between the lines of defence, and the prevention of possible 'blind spots';
- The use of combined assurance to support the audit committee and board in making their control statements in the integrated report; and
- A comprehensive and prioritised approach to the tracking and testing of remedial actions on identified improvement opportunities, control weaknesses or significant inherent risk mitigations.

While combined assurance offers numerous benefits, it seems to be a challenge for commercial companies to embed the process. That which your business has in place to protect itself can be measured against the four lines of defence described above. They form a critical part of the organisation's overall response to risk. Some of the business challenges that prevent companies from responding effectively through their lines of defence include:

	Business challenge	Recommended action	What you gain
1	Inadequate culture and behaviour at the top	• Lead by example. The tone at the top is where everything begins. • Pride of ownership, personnel-wide understanding of organisational strategy and a well-embedded organisational culture will drive performance across the organisation. • You may consider a 'cultural assessment' to identify areas for improvement and to measure corporate behaviour.	• The right tone at the top is a strategic driver of performance: In building the right high-performance culture, opportunities and resilience will emerge, ultimately future proofing your organisation against risk.
2	Lack of balance between risk resilience and readiness	• Take a broader, more holistic perspective and adopt a future-facing approach towards risk to become a strategic driver of performance. *Risk is everyone's responsibility!* • Challenge your lines of defence to think more holistically about your key risks and assist in adopting a different mindset around opportunities presented by risk, as much as the threats. • Mobilise your lines to navigate through your risk landscape, assessing and uncovering risk and opportunities.	• Thinking differently about risk will bring commercial advantage and the ability to plan ahead with certainty, while adapting to change in the knowledge that you have taken essential steps to counter the 'yet to come'. • An ability to react quicker on unknown risks and leverage opportunities in advance will give you a competitive edge and the ability to use your lines of defence as a growth enabler.
4	Lack of board confidence in the effectiveness of governance, risk and control processes and the quality and reliability of management reporting	• *Get your board on board* to improve the quality and reliability of reporting on risks and opportunities to the board by management across the lines. • Strengthen independent assurance on critical risks across the lines.	• Increased confidence in the quality of management reporting enables the board to leverage the model to better manage risks and create opportunities, thereby using the model as a growth platform. • Boards are able to gain a holistic view of the business risks and opportunities and have more comfort and peace of mind on the critical risks being assured. • A comprehensive and prioritised approach in tracking and testing remedial actions on identified improvement opportunities, control weaknesses or significant inherent risk mitigations.
5	A blurred lines-of-defence model, resulting in irrelevant, inefficient and inadequate co-ordination of assurance efforts	• Demystify and identify your assurance providers. Get an understanding, through co-ordination between the lines of defence, of who is providing assurance over critical risks. Are the right risks being assured by the right assurance providers? An 'assurance map' may be considered to identify possible areas of assurance fatigue or redundancy, or areas 'falling through the cracks'. • Break the silence across the lines of defence – Interaction and co-ordination are key across the four lines of defence. Let them break the silence between them, and let them voice and co-ordinate their efforts – who is assuring what and when?	• Optimally co-ordinated and relevant assurance efforts focusing on key risk exposures and assessing whether the organisation will be able to execute its strategies successfully to achieve its objectives. • Optimise assurance spend by assisting external providers of assurance to give opinions on residual risk status; prevent assurance fatigue; minimise overlap between the lines of defence; and prevent possible 'blind spots'. • Minimise business/operational disruptions by achieving adequate co-ordination between the various lines of defence.

Step 1: Complete an assurance map

Based on our hands-on experience in assisting companies in the commercial industry with the embedding of combined assurance, we set out below a practical approach to implementing an effective combined assurance approach.

The foundation for combined assurance and the successful implementation of a combined assurance model rests on the quality of the risk management information. Poor risk definitions, missing critical risk information, no risk taxonomy and poor control mitigation information will negatively affect the implementation of combined assurance.

The first step in the process is completing the assurance map by indicating who assures what risk and to where this assurance is reported.

Risk Number	Risks	Line 1				Line 2				Line 3		Line 4	
		People and process		Management supervision and oversight		Risk management		Compliance		Internal audit		Independent external assurance	
		Actual	*Proposed*	*Actual*	*Proposed*	*Actual*	*Proposed*	*Actual*	*Proposed*	*Actual*	*Proposed*	*Actual*	*Proposed*
1	Financial sustainability												
2	Legal and regularity compliance												
3	Competitive position												
4	Brand integrity											Not applicable	
5	Theft, fraud and corruption												

This step in establishing an effective combined assurance approach will require the most effort and is likely to take a relatively long time to complete. The detail is vital to ensure that combined assurance delivers its potential value to the organisation. It will also set the foundation for considering other assurance efforts that may be introduced in the future. For example, a culture and climate survey should address identified risks where this sort of assurance is required.

Step 2: Assurance reality check

The profile developed in step 1 only establishes the foundation for further work on combined assurance. Now the challenge is to assess the actual assurance provided and to whom the assurance is provided. The quality of the assurance should also be assessed through interaction with the recipients of the assurance and assessment of the reports issued.

Assurance is provided primarily by the second, third and fourth lines of defence (see Annexure I for a brief description of the lines of defence). While management do provide extensive risk assurance through performance management and reporting, this is not factored into combined assurance, as it would require comment/evaluation on the effectiveness of management in this regard. Their activities will, however, be considered where no second, third or fourth lines of defence are considered appropriate in the combined assurance model.

Assurance reality check

The auditing of the assurance providers is essential to establish what is being done and for what reasons. It can also provide valuable information on the investment the organisation is making in assurance and provides an opportunity to evaluate the returns it receives - is the assurance quality and coverage worth the cost?

Step 3: Combined assurance design

Steps 1 and 2 establish what assurance is provided and present a recommended approach to address the gaps in desired assurance. All stakeholders involved now need to be convinced of the approach and their respective responsibilities.

What assurance is to be provided to whom

This step identifies the recommended area of assurance and needs to articulate the nature of the assurance activities.

Acceptable methodology/credibility

The assurance provided must be credible. This is achieved by ensuring that the skill and experience levels of the assurance providers are appropriate for the work to be performed, and that the extent of the work performed will address the potential and actual exposures.

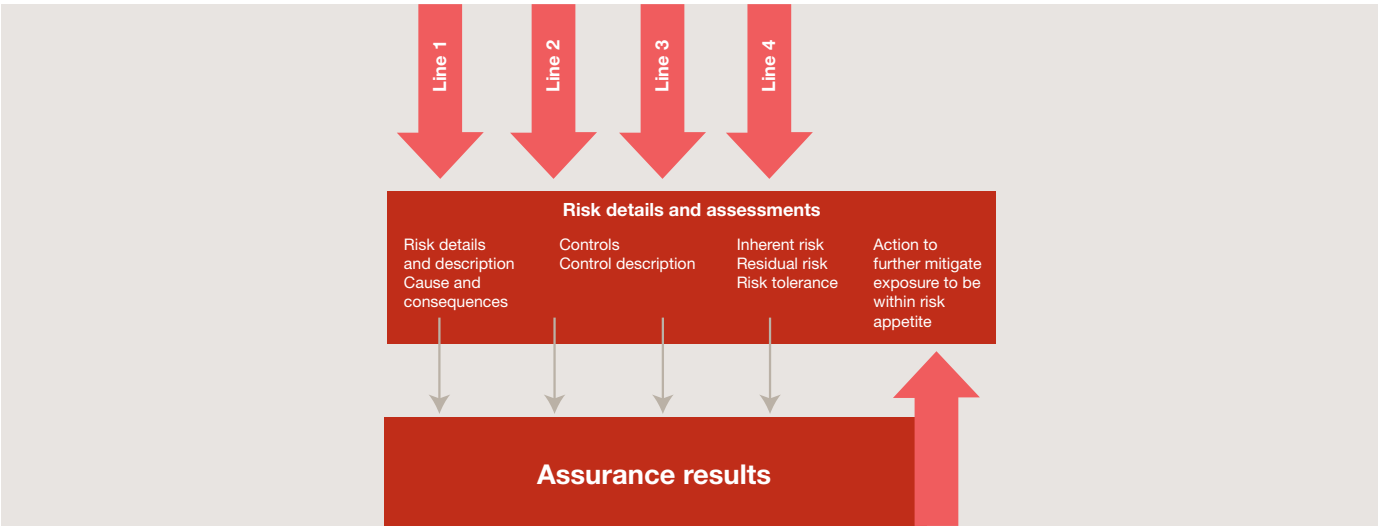
Management and the board will need to ensure that the assurance providers appointed – both external and internal – have the appropriate experience and skills and follow an acceptable approach/methodology.

The key output from step 3 is the blueprint for combined assurance. This will include the risk-based assurance coverage, analysed per assurance provider and management/ governance committee responsible. It should include the frequency and extent of assurance required.

Ultimate acceptance of the blueprint will need to be championed by the executive sponsor and will require extensive consultation with the operations, executive and governance committees and ultimately the board or its equivalent.

Ownership of the blueprint must also be determined. King III requires the audit committee to oversee the combined assurance approach, and it is then the natural owner of the blueprint. From an operational point of view, internal audit or risk management is well positioned to review the continued relevance of the blueprint and suggest updates in the future.

Understanding the combined assurance provided and the roles of the assurance providers.



The combined assurance blueprint

Combined assurance can successfully be applied at project or programme level. The value in project / programme assurance is improving performance and efficiencies; cost and recovery optimisation, and risk avoidance and management according to pre-defined success and failure factors to improve delivery confidence for the project/ programme stakeholders.

Portfolio

- Portfolio level

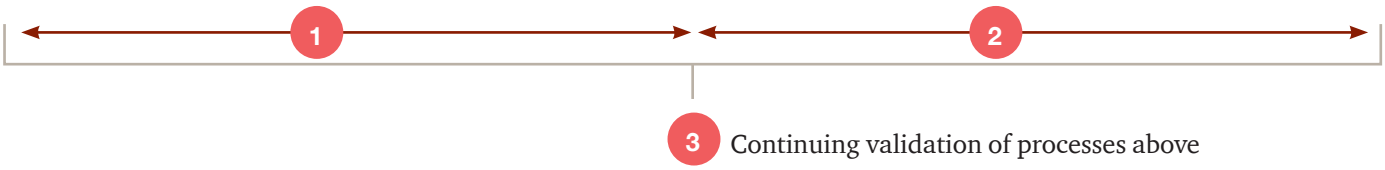
Programme

- Programme level

Projects

- Project 1
- Project 2

Risks	Qualification measurement	Risk mitigation	Assurance level 1	Assurance level 2	Assurance level 3	Assurance level 4
Project risks	Inherent risk Residual risk Risk tolerance	Planned control framework	Management	Risk management compliance	Internal audit	Independent external assurance



1. Gathering all the data – establishing the baseline
2. Assessment of actual assurance and mapping of risks – including reporting

The challenge is to align the assurance activities and to report on the status of assurance provided. The automation of the process is an effective way to co-ordinate the activities and to ensure consistent reporting for the different types of assurance provided.

Step 4: Making combined assurance a continuing reality

Internal Audit or Risk Management are usually best placed to take on the combined assurance champion role. They have an overall understanding of the business, are familiar with the assurance concepts and have a strong vested interest in making sure the approach is effective. Other second-line-of-defence functions can take on the championing role, such as Compliance, the Company Secretary, and Legal.

The on-going co-ordination of the combined assurance efforts can be achieved through a Combined Assurance Forum (CAF).

The Combined Assurance Forum will comprise a minimum of a representative of the external auditors, internal auditors, governance/sustainability assurance providers, legal services and representatives of the GRC function (governance, risk and compliance). Members of this Forum will be nominated by GRC. The members of the Combined Assurance Forum should represent the different assurance providers within the group and be of sufficient seniority to be able to make decisions on behalf of the assurance function.

The diligence and effort in establishing an effective combined assurance approach must be matched by on-going efforts to ensure the approach provides the value it is designed to provide.

Our practice has found that activating the assurance reporting on the risk management platform provides the lasting solution.

Assurance providers plot their assurance activities planned against the risk profile. The risk and process owners can then assess the extent of disruption and overlap together with the Combined Assurance Forum.

- The assurance assessment on residual risk status is recorded for the risks with a URL link to the assurance report s etc.
- The assurance assessment can be compared to management assessment of residual risk.
- Assurance findings are recorded as actions per the risk management system and remediated according to overall priority of all recorded remediation. Action tracking will apply equally to those findings.
- Management and the Board then have access to “real time” assurance and do not have to wait for the audit process to be completed.
- Assurance reporting is a couple of key strokes away at any time as required.

How we can help you

PwC has invested substantially in risk management solutions, both locally and globally. Our experience and hands-on expertise ensure that this investment can be practically applied for our clients' benefit in a number of ways:

- Advising on risk governance and risk management plans;
- Articulating risk appetite and tolerance;
- Linking performance and risk management;
- Developing effective risk management frameworks and methodologies;
- Facilitating risk assessments;
- Benchmarking risk and risk mitigation activities;
- Addressing ICT risk management;
- Advising and providing solutions on compliance risk;
- Assisting in embedding risk management;
- Assessing the effectiveness of risk management;
- Assessing current assurance providers in terms of their existence and effectiveness;
- Developing a combined assurance profile and risk governance reporting framework;
- Developing an integrated capital project assurance framework;
- Performing capital project and portfolio risk assessments; and
- Creating a fraud risk response plan together with management.

Critical success factors of the combined assurance model

- The board is responsible for ensuring that business-critical risks are being assured and adequately managed. The four-lines-of-defence model strengthens independent assurance reporting to the board and senior management on the critical risks facing the company. There should be adequate buy-in and cultural support for this model at the top.

- A fundamental foundation of the four-lines-of-defence model is effective risk management and mature risk management processes. This is further driven by the tone, culture and buy-in at the top and how this resonates with everyone in the company who is responsible for the management of risk. *It is everyone's responsibility!*

- It is key to define and clarify the levels of independence and how they are strengthened across the four lines. In addition, the definition of assurance, and what it is that is actually assured over the four lines, should be clearly understood. It can even be to the extent that roles and responsibilities across the company in terms of the four lines of defence are defined in policies, procedures, job descriptions, delegations of authority, etc. to make the concept more understandable and the model easier to implement and monitor.

- There must be adequate co-ordination between the four lines of defence. For the model to be effective, line four should in reality be able to rely on lines one to three. The extent to which line four is utilised is highly dependent on the company's risk appetite and the level of assurance comfort required by the board, or whether there are regulatory requirements, such as the annual statutory audit. If the inherent risk is considered to be high and lines one to three cannot provide this heightened level of assurance, or the company simply does not have the skill or resources to provide this assurance, additional independent assurance may be required by the board.

- An understanding is needed of who the assurance providers in the company are, and the assurance providers must be aligned to the critical risk exposures. A*re the right risks being assured?* Assurance is provided by a broad range of departments, differentiated by the stakeholders served. An 'assurance map' may be considered to identify possible areas of assurance fatigue, redundancy or areas 'falling through the cracks'.

Annexure I:
Lines of defence

Without a cohesive, integrated and co-ordinated approach, the organisation cannot co-ordinate essential risk management roles and responsibilities. In the four-lines-of-defence model, each line plays a distinct role within the organisation's wider risk and control framework.

The first line of defence should own the risks and controls. This includes management supervision and oversight.

The second line of defence should monitor these risks and controls. The second line should be working directly with the business to define and drive the risk management framework and the internal control structure as part of the day-to-day operations and oversight of the company.

The third line of defence is generally internal audit, which is internal to the organisation. Internal audit by nature and definition, according to the Institute of Internal Auditors (IIA), should be objective and independent and should provide assurance over the company's adequacy and the effectiveness of its internal controls, risk management and governance. This therefore includes the activities of the first and second lines of defence. The strength of internal audit's independence is measured through a direct functional reporting line to the Chairperson of the Audit Committee and administratively to the Company Chief Executive Officer. If the lines between the second and third lines of defence blur, the safety net for senior management and the board becomes less effective and may not enable the board to fully discharge its governance oversight responsibility.

The fourth line of defence introduced by the combined assurance model consists of all external assurance providers who are completely independent of the company. This includes the external auditors, the regulators and any other external body outside the company's structure. They have a very important role in the company's overall governance and control structure. This is particularly relevant in highly regulated sectors such as those of financial services or insurance. External audit provides the shareholders with assurance, but also delivers valuable information to the company around financial risk and reporting, especially to the board and senior management. External auditors may also be required to perform non-audit services, but this depends on the company's board and whether there is an appetite for this. There could very well be restrictive policies within the company prohibiting the external auditors from providing any assurance activities other than the statutory audit.

Understanding the assurance provided through the combined assurance model:

First line of defence	Second line of defence	Third line of defence	Fourth line of defence
Management oversight	**Management of risk and compliance**	**Internal audit**	**Independent external assurance**
Nature of assurance	***Nature of assurance***	***Nature of assurance***	***Nature of assurance***
Line management are accountable and responsible for the management of risk and performance. A key element of this line of defence is the extent of management reviews and the actions that follow. Management can establish a system of self-assessment/ audits to inform them of the adequacy of risk management activities.	Corporate functions provide support to line management in executing their duties. These typically include functions such as human resources, procurement, compliance, risk management, quality assurance, health and safety, SOX, tax, engineering, forensic (fraud risk management), insurance and actuaries.	Internal risk-based audits that provide independent and objective assurance over the controls, risk management and governance activities of the company as performed in lines one and two. Internal audit may also provide combined assurance with line two on activities in line one, or combined assurance with line four on activities in line one and two. Should the inherent and residual risk be high, lines two and three may review the same areas.	External assurance providers such as certifications, regulator reviews, external audit, technical audits, forensic investigations, external asset management reviews, valuators, culture climate surveys, assessments of ore/mineral reserves, etc.
• Examples of activities • People and process, management supervision and oversight. This would also include technology. • Responsibility and accountability for managing risk around business-as-usual • Incentivised to manage risks and remediate issues • Ensure that controls are performed properly in the first place – not post-event control assurance • Appropriate mix of preventative and detective controls • Good integration with an appropriate suite of monitoring controls	• Examples of activities • Risk and compliance functions – not bits of finance, human resources, etc. • Defining, setting and maintaining risk management policies • Promotion of risk awareness • Advising line one on how to manage risks • Facilitating/Governance of risk and controls self-assessments to identify and measure risks and assess related controls • Monitoring of key risk and control indicators • Monitoring of losses • Performing targeted deep dives • Tracking remediation/risk acceptance of issues • Scenario planning and stress testing • Managing of incidents • Providing portfolio, programme/project oversight and quality assurance	• Examples of activities • Risk-based internal audits • Risk management reviews • Compliance with policies and procedures • Corporate governance reviews • Specific ad hoc reviews requested by management • Consulting services – *however, these services pose a potential threat to independence and all consulting activities allowed to be performed by internal audit should be clearly defined in the internal audit charter.* • Combined technical audits with line four, making use of external specialists. In certain instances, internal audit may also use resources from lines one and two to assist with a specific audit. This is the so-called '*guest auditor*' principle.	• Examples of activities • Statutory external audits. In certain instances, external audit may also rely on internal audit's work. • Certification services such as ISO certification • Technical audits such as providing project assurance to a third party • Valuations of property, plant and equipment • Combined technical audits with internal audit

First line of defence	Second line of defence	Third line of defence	Fourth line of defence
Reporting lines	***Reporting lines***	***Reporting lines***	***Reporting lines***
• Executive management and operational committees providing direction, guidance and oversight over the focus areas	• Risk committee • Compliance committee • Audit committee • Regulatory forums • Human resources forums • Health and safety briefings	• Regulators • Board and audit committees • C-Suite	• Regulators • Board and audit committees • C-Suite • Public

Annexure II:

Criteria for assessing assurance providers

Objective

The objective of this section is to provide an overview of the requirements that need to be satisfied in order to allow internal audit to place reliance on the work done by other assurance providers. These requirements are guided by the International Standard on Auditing 620, 'Using the work of an expert'.

Scope

This section focuses on the assurance being provided in technical/specialist fields.

Requirements to qualify as an assurance provider

Category	Minimum requirements
Independence/Objectivity	Independent reporting lines, no recent direct involvement and/or work done in the area/aspects to be audited
Conflict of interest	In the areas/aspects in which assurance is to be provided, there should not be any conflict of interest (could require a declaration in this regard).
Skills and experience	The assurance provider should have the appropriate skills and experience to effectively conduct the assignment.
Qualification	The assurance provider should hold an appropriate qualification(s).
Assurance methodology	A sound audit/review methodology should be adopted by the assurance provider. Ideally, a risk-based approach should be followed. The reported findings and opinions should be supported by adequately documented working papers/audit trails.
Accreditation body/Registration *(non-core aspect)*	Ideally, the assurance provider should be accredited or registered with a recognised accreditation body for the areas/aspects over which he/she is providing assurance.

Annexure III:

Contact details

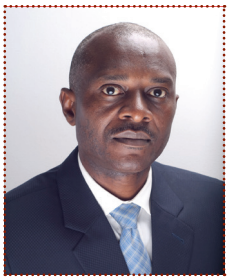
Anton van Wyk
Risk Assurance Leader – Africa
Partner
(011) 797 5338
083 300 4900
anton.b.van.wyk@za.pwc.com

Shirley Machaba
Risk Assurance Leader – South Market
Partner
(012) 429 0037
082 497 1077
shirley.machaba@za.pwc.com

Dalene Rohde
Associate Director
(012) 429 0066
082 771 1506
dalene.rohde@za.pwc.com

Rob Newsome
Risk Assurance Leader – Nigeria
Partner
Direct :+234 (1) 271 1700 Ext 3100 ,
Mobile: +234 8189036007
rob.x.newsome@ng.pwc.com

Mark Telfer
Risk Assurance Leader – East Africa
Partner
(011) 797 4628
082 454 6862
mark.telfer@za.pwc.com



Michael Asiedu-Antwi
Partner – Ghana
+233 302 761 500
0277-277277
michael.asiedu-antwi@gh.pwc.com

Andre Goosen
Senior Manager
(011) 797 4979
072 565 0049
andre.goosen@za.pwc.com

Ferdi Linde
Senior Manager
(011) 797 5195
073 588 7036
ferdi.linde@za.pwc.com