

Preparation. Perseverance. Payoff.*

Implementing a combined assurance
approach in the era of King III



Contents

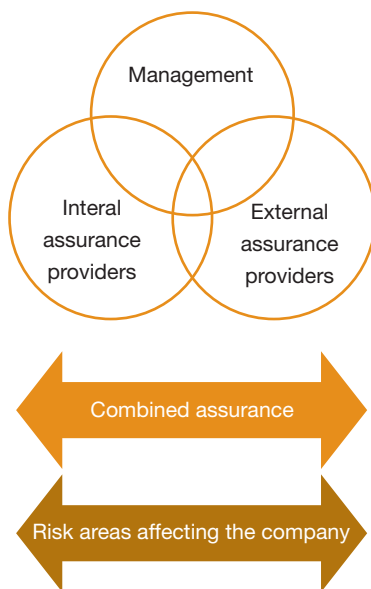
Combined assurance and corporate governance	4
Step 1: Establishing the business case	4
Step 2: Assurance reality check	6
Step 3: Risk mapping	7
Step 4: Combined assurance design	10
Step 5: Making combined assurance a continuing reality	11
Where does external audit play a role?	12
The take-away message	12
How we can help you	13
Appendix I: Lines of defence	14
Appendix II: Example assessment of assurance provider	15
Appendix III: Criteria for assessing assurance providers	18
Appendix IV: Contacts	19

Combined assurance and corporate governance

“The audit committee should ensure that a combined assurance model is applied to provide a coordinated approach to all assurance activities”¹

Principle 3.5 of the King Report introduces combined assurance as a recommended governance practice. The recommendation has been made following a general understanding that more can be done to improve assurance coverage and quality through better co-ordination of the assurance providers.

Combined assurance model ²



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:

- Coordinated and relevant assurance efforts focusing on key risk exposures;
- Minimised business/operational disruptions;

The King Committee on governance issued the King Report on Governance for South Africa – 2009 (the “Report”) and the King Code of Governance Principles – 2009 (the “Code”) together referred to as “King III” on 1 September 2009.

- 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 being reviewed by the different committees;
- Possible reduced assurance costs; and
- The use of combined assurance to support the audit committee and board in making their control statements in the integrated report.

While combined assurance offers numerous benefits, it is one of the biggest challenges facing businesses and organisations in adopting King III. Based on our hands-on experience in implementing the combined assurance model in organisations, this paper sets out a practical five-step approach to implementing an effective combined assurance approach.

Step 1: Establishing the business case

The business case should be clearly established through a high-level understanding of what assurance is provided for the risk exposures facing the enterprise.

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

The business case is established through getting an overview status of the assurance profile.

The profile can be established through a process view of activities and mapping the possible/actual assurance providers to the process type view. An example is set out in the table that follows.

¹ *Third King Report on Governance for South Africa – 2009*. (Johannesburg: Institute of Directors in Southern Africa, 2009) 62.

² *Ibid.*

Processes assurance assessment

Processes	Three lines of defence assurance providers											
	First line of defence			Second line of defence				Third line of defence				
	Management-based assurance			Risk and legal-based assurance				Independent assurance				
	Control self assessment	Special project	Management review	Risk management	Health and safety	SOX	Compliance	External audit	Internal audit	ISO certification	Consulting engineers	Special project
Strategic												
Cash/finance and treasury												
Funding												
Sustainability												
Growth / mergers & acquisitions												
Alliances												
Operational												
Financial												
IT												
Treasury												
Human resources												
Supply chain management												
Quality												
Environment												
Customers												
Products & services												

Key:

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

This profile can be used to assess the potential for combined assurance – gaps, duplication, curiosity for further detail and King III compliance. The audit committee should use this profile to commission further work on establishing combined assurance. At this point an executive sponsor should also be identified to ensure that co-operation is provided for the initiative throughout the business/operations.

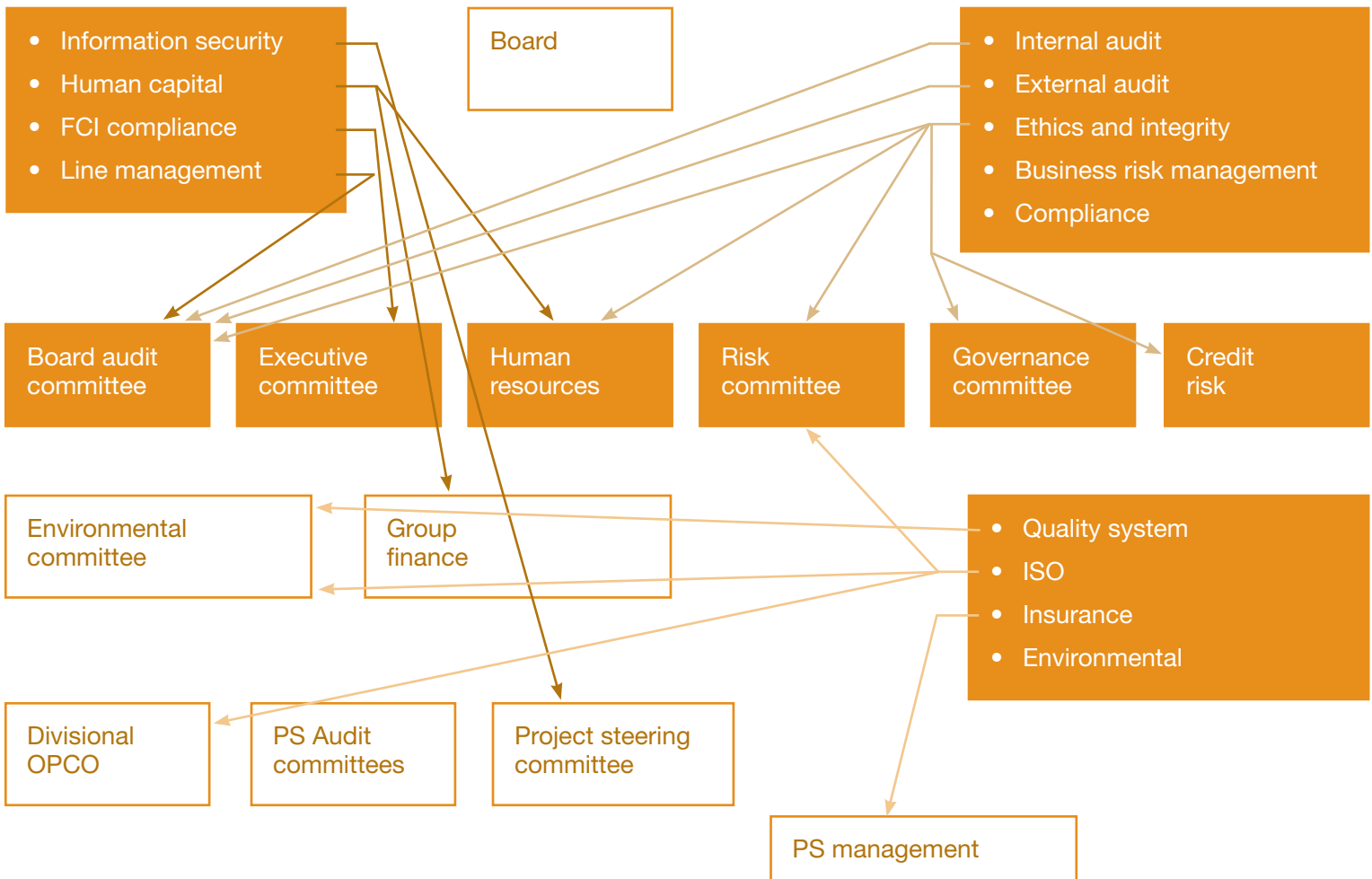
Step 2: Assurance reality check

The profile developed in step 1 only establishes the case 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.

The following diagram illustrates a possible current state of assurance reporting to management and the governance structures. Often this assurance is uncoordinated and duplicated:

- Assurance may never reach the appropriate forum – for example key engineering assessments at a mine level never leave the mine;
- Some forums do not receive any assurance – for example project management committees;
- Certain governance committees are overburdened with assurance – for example the audit and risk committees; and
- Board and executive agenda items are also debated and considered in the board subcommittees.

Assurance reality check



The audit of the assurance providers is essential to establish what is being done and for what reasons. This step also identifies the assurance sponsors that need to be consulted to make combined assurance a reality. This co-operation may need to be prioritised by executive management to address vested interests.

The assurance providers can include:

- Internal audit
- External audit
- Ethics and integrity
- Business risk management
- Compliance
- Information security
- Human capital
- SOX compliance
- Quality system
- ISO 14001
- ISO 9001
- HACCP
- Insurance
- NOSA
- Owner manufacturer inspections
- Special projects

Internal audit is well placed to complete the assurance reality check. It can assess the quality of assurance provided and the relevance to the management or governance committee.

The 'audit of the auditors' provides further information about the overall actual investment the entity is making in assurance and provides an opportunity to evaluate the returns received: **is the assurance quality and coverage worth the cost?** This will further support the business case for progressing to the next steps of the combined assurance approach.

Step 3: Risk mapping

The universe for assurance needs to be clearly established in order to fully understand what assurance is currently being provided and what needs to be provided.

The strategic, key operational and business unit-level risk profiles should be used to establish what risks are assured and by whom and what risks should be assured and by whom. This step will allow a detailed gap analysis to be developed and to inform the next step of the required investment.

In the analysis, the different lines of defence will be mapped to the identified risks in terms of work actually performed and the assurance expected.

The profile can be updated following step 2, in which the assurance providers are identified and their plans and reports reviewed.

Ideally, the data should be captured on risk management or other suitable software to allow analysis and reporting from the data established – for example, detailing the risks covered by specific assurance provider versus the assurance that is recommended.

The chart that follows on the next page illustrates the detail required to make a realistic assessment of the actual and desired assurance. This step does require detailed work to analyse and capture the existing assurance and to inform recommendations. Again, internal audit is well placed to lead this analysis. It has the training and experience to understand the risks and associated controls/risk mitigation measures and how the assurance relates to these profiles.

Risk map

Risk for each risk management function	Associated controls	Three lines of defence assurance providers		
		First line of defence		
		Management-based assurance		
		Control self assessment	Special project	Management review
Procurement process				
Supplier management				
Contracts master maintenance				
Purchase requisitions				
+ Purchase orders and contracts				
Production scheduling and purchasing not integrated	• Document production schedules and material requirements;		√	
	• Define documentation standards for production schedules and material requirements; and			
	• Integrate the production scheduling system with the purchasing system.		√	
Orders are not supported by authorised requisition	• Align purchase orders and inventory levels;	√		
	• Periodically reconcile production needs with purchase orders and inventory levels to ensure they are adequately aligned; and	√		
	• Require an authorised requisition for all purchase orders.	√		
Long-term needs are not analysed	• Analyse long-term needs and establish forward contracts with standing orders	√	√	
	• Contracts performance to meet needs identified must be monitored and corrective action taken timeously.	X		
Excessive inventory levels	• Manage inventory levels optimally so as to reduce associated costs; and	√		
	• Evaluate the use of electronic data interchange (EDI) for placing orders directly into the supplier's order entry system.			
Purchase orders/ inventory levels not reconciled with production requirements	• Configure the computer system to automatically generate purchase orders based on material requirements, current stock levels, and previously specified desired minimum stock levels; and	X		
	• Periodically reconcile production needs with purchase orders and inventory levels to ensure they are adequately aligned.	√		
Tendering process				
Receiving and distribution of goods and services				
Vendor invoice verification				
Payments				
Documentation management				

No assessment of the adequacy of management review

Key:

 Currently providing assurance

 Should provide assurance

√ Quality of assurance acceptable

x Quality of assurance unacceptable

This step will require the most effort to establish an effective combined assurance approach and is likely to take a relatively long time to complete. This detail is vital to ensure that combined assurance delivers its potential value to the organisation. It will also set the foundation for consideration of 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 4: Combined assurance design

Step 3 establishes what assurance is provided and presents a recommended approach to address the gaps to desired assurance. All stakeholders involved now need to be convinced of the approach and 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.

Example:

Biannual mine visits by independent consulting engineers to verify progress against mine plan. The assurance will be reported to Exco, which will report to the board on the assessment completed. This may also be included in the integrated report (annual report).

Agreeing a common universe

The risk profile must be established in a manner that is relevant to the business/operations and is managed on a consistent basis. Risk information is often maintained independently in the different business/operational units or by the assurance providers.

Example:

health & safety officials may identify risks based on specific relevant risks and rated on a numeric severity rating. In contrast, internal audit may maintain a risk assessment based on monetary value.

The integrated risk management approach recommended by King III should provide the foundation for the establishment of the assurance universe, thereby providing a sound base for establishing the assurance footprint.

Acceptable methodology/credibility

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 ensuring that the extent of the work performed will address the potential and actual exposures.

In the above example, a team of consulting engineers may well have the skills necessary to review the mine plan, but if they do not follow acceptable survey techniques, their work may not be credible in providing the required assurance.

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 4 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 through the operations, executive, governance committees and ultimately the board or 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 is well positioned to review the continued relevance of the blueprint and suggest updates in the future.

Step 5: Making combined assurance a continuing reality

A combined assurance champion must be identified to implement the approach. Ideally, there should be an executive sponsor who is able to provide the required authority for the project. The executive sponsor should be the person to whom the champion functionally reports.

Internal audit or risk management is usually best placed to take on the combined assurance champion role. They have an overall understanding of the business and 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 champion role such as compliance, the company secretary, or the legal function.

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

King III requires internal audit to provide assessments of internal control (including internal financial controls) to the audit committee. Given the diversity of risks and controls required, internal audit cannot realistically

provide this assessment without considering and relying on the combined assurance approach. Internal audit could provide its assessment of internal control by reporting on the adequacy of assurance provided by the implementation of combined assurance. Internal audit will need to assess the continued adequacy of the design of the combined assurance blueprint as well as how well the assurance has been provided.

Clearly internal audit can provide an assessment of the adequacy of assurance provided over its own work. However, it will also need to assess the adequacy of work covered by other assurance providers. Internally it may need to assess the assurance coverage, methodology followed and adequacy of reporting based on the evidence obtained.

Externally, this may not be easily achievable – internal audit will need to evaluate the extent to which it can rely on third parties. External auditors have developed standards that need to be followed in situations where they rely on third parties. Internal auditors will need to develop equivalent standards/guidelines. In the interim they can borrow from external auditors.

Note: The Institute of Internal Auditors' (IIA) standards require that internal audit completes an external quality review of their work at least once every five years. This quality assurance provides an assessment of the effectiveness of the internal audit function.

Where does external audit play a role?

The external auditor's understanding of the broader business risks and knowledge of how to provide robust assurance means that they can perform a valuable role in a combined assurance framework. External auditors have experience of best assurance practice in different sectors and companies. Their detailed knowledge of good governance frameworks, such as COSO, can be used in the design of the assurance framework. Drawing on their understanding of the broader business risks and how to provide robust assurance they can:

- Share insight of where assurance works well/not so well in other sectors and companies; and
- Provide expertise in risk and assurance mapping, helping to identify:
 - Gaps in the combined assurance framework (i.e. where there are currently risks or controls which may not be adequately mitigated);
 - Areas of overlap between different assurance providers (which can be eliminated to yield cost savings);
 - Areas in which the quality of the assurance provided is insufficient (i.e. where a function nominally provides assurance but the testing is not sufficiently robust or rigorous); and
 - Areas in which assurance on other providers can be placed and how this progresses from time to time.

The take-away message

The implementation of a combined assurance model will take time and effort to establish and maintain. However, this time and effort are insignificant compared with the potential benefits, which include:

- Reducing assurance fatigue through better co-ordination;
- Providing priorities for remediation;
- Improving the value of assurance; and
- Enhancing corporate governance practices.

Those charged with governance of any entity should actively ensure that an effective combined assurance approach is established and maintained.

How we can help you

PricewaterhouseCoopers 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 – existence and effectiveness;
- Developing a combined assurance profile and risk governance reporting framework; and
- Creating a fraud risk response plan together with management.

Appendix I: Lines of defence

International corporate governance trends and best practices are highlighting the importance of effective combined assurance across the following lines of defence:

First line of defence:

Management oversight including strategy implementation, performance measurement, risk management, SOX internal control, company control; and other control and governance processes, including, control self-assessment, and continuous monitoring mechanisms and systems.

Second line of defence:

Enterprise risk management operating a formal, robust and effective risk management framework within which the entity's policies and minimum standards are set, with objective oversight and ongoing challenging of risk management performance and reporting being achieved across the entity. Legal, compliance, health and safety, and quality assurance are often included in this line of defence.

Third line of defence:

Independent and objective assurance of the overall adequacy and effectiveness of risk management, governance, and internal control within the entity as established by the first and second lines of defence. This is predominately the role of the audit committee, supported by internal audit, external audit and other credible assurance providers.

Appendix II: Example assessment of an assurance provider

Assurance provider	Health & safety (H&S)
Assurance lead contact	VP/head of H&S
Nature of assurance	<p>To provide reasonable assurance that:</p> <ul style="list-style-type: none">• An effective H&S management system has been defined, set up and implemented group wide;• The H&S management system is actually operative in each of the group's entities;• Targets and objectives are set up at both corporate and entity levels in consideration of objectives for continuous improvement;• The H&S management system performance, at corporate and business unit levels, is measured and necessary remedial actions are identified, undertaken and monitored;• The financial statements and related group consolidation is fairly represented and free of any material errors, omissions and misstatements.

How is assurance provided	Risk category	Scope and approach	Planned reviews	How is assurance measured
Corporate H&S organises regular self assessment addressed to all business units	Legal & compliance and health & safety	The board has adopted an H&S policy and management system that has to be implemented deep into the organisation. Corporate H&S monitors the effectiveness of the H&S management system.		<ul style="list-style-type: none"> • Number of self assessments performed; • Average score of all assessments; and • Number of recommendations made to CEOs for improvement
The group has adopted the OHSAS standard and has set objectives for business units to be “OHSAS certified”.	Legal & compliance and health & safety	OHSAS provides through the ISO14001 standard the ingredients for a strong and efficient H&S management system. The group has adopted this standard with the objective to eventually have each industrial business unit certified for this standard.		<ul style="list-style-type: none"> • Number of business units actually ISO14001 certified against the total objective; • Number of OHSAS pre-audits performed by H&S internal auditors in preparation of the official certification; and • Number of business units to be certified within the coming 12 and 24 months.
Reporting of accidents or near misses as a measure of the actual H&S management system performance	Legal & compliance and health & safety	Sharing information about losses experienced is essential to monitoring the risk of accident. The group has set up a platform for exchanging this information between all parties involved within the group regardless of their location.		<ul style="list-style-type: none"> • Number of reports published; and • Number of visitors to the platform to read these reports.
Accident ratios are computed, published and commented upon. Objectives are set up at group and business unit level	Legal & compliance and health & safety	A universally accepted way to measure H&S performance is to compute and publish accident ratios. These are to be compared and commented on frequently. Objectives must demonstrate that the strong involvement of the board to achieve a “zero accident” rating is taken into consideration.		<ul style="list-style-type: none"> • Group accident ratios and trends; • BU’s accident ratios and trends; and • Number of H&S meetings at group level.

Type of reporting	Format	Source of data / information	Frequency of reporting	Report distribution
Self assessment reporting for H&S management system implementation	<ul style="list-style-type: none"> • Formal written report; and • Presentation 	Self assessment results	6 monthly	<ul style="list-style-type: none"> • Audit committee members; • Board members; • Executive/senior management; and • Unit management
Cost of assurance	Budget:	R	Anticipated final cost:	R

Source: ArcelorMittal Corporate Internal Assurance

Appendix III: 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).
Skill 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/aspect over which he/she is providing assurance.

Appendix IV: Contacts

Gauteng

Akhter Moosa

Director

(012) 429 0546
082 771 1275
akhter.moosa@za.pwc.com

Shirley Machaba

Director

(012) 429 0037
082 497 1077
shirley.machaba@za.pwc.com

Rob Newsome

Director

(011) 797 5560
083 611 8500
rob.newsome@za.pwc.com

Dalene Rohde

Associate Director

(012) 429 0066
082 771 1506
dalene.rohde@za.pwc.com

Cape Town

Steve Roberts

Director: Risk Advisory Services

Tel: +27 21 529 2009
E-mail: steve.m.roberts@za.pwc.com

Durban

Shirley-Ann Bauristhene

Director: Risk Advisory Services

Tel: +27 31 271 2007
E-mail: shirley-ann.bauristhene@za.pwc.com

East London

Frank Muller

Associate Director: Risk Advisory Services

Tel: +27 43 707 96668
E-mail: frank.muller@za.pwc.com

Bloemfontein

Connie Hertzog

Director: Assurance

Tel: +27 51 503 4100
E-mail: connie.hertzog@za.pwc.com

Polokwane

Glory Khumalo

Director: Assurance

Tel: +27 15 291 0100
E-mail: glory.m.khumalo@za.pwc.com

Nelspruit

Pierrie Cronje

Director: Assurance

Tel: +27 13 754 3511
E-mail: pierrie.cronje@za.pwc.com

