A combined assurance model, is it something everyone should aspire to?

By Oliver Laloux
Mondial Risk and business consultants

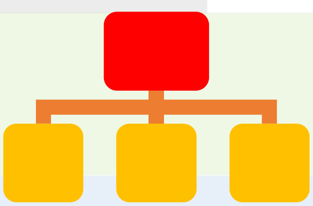
Recent developments in the risk and assurance fields have resulted in many discussions, especially at the Board sub-committee levels, around integrated and combined assurance models (hereafter referred to as CAM).

The official publication of the King IV Report on Corporate Governance for South Africa (the "King IV Report") in late 2016 has rejuvenated many of these discussions, often with a limited understanding of what an integrated and combined assurance model really involves and requires in practice. The latest definition of combined assurance proposed by King, that it recommends but does not prescribe states:

"A combined assurance model incorporates and optimises all assurance services and function so that taken as a whole, these enable an effective control environment; support the integrity of information used for internal decision making by management, the governing body and its committees; and support the integrity of the organisation's external reports."
King IV Report 2016.

A mouthful, with reference to incorporation, optimisation, integrity, decision making and an effective control environment. The word missing in the definition but referenced in many other places in King IV and related publications is that for CAM to add value, it should be <u>risk based</u>. In addition, we now all must apply AND explain and not just apply or explain.
So, what does this mean to decision makers on 'governing bodies' and its sub-committees? What can they reasonably expect from management when it comes to a CAM? And more importantly, what level of risk, assurance and organisational maturity is required to make CAM work. We attempt to answer some of these questions and to open honest debate as to what are the underlying factors that need to be in place before management is tasked with developing and implementing a CAM.

In order for CAM to work and be implemented, based on our practical experience, we propose that a number of things need to exist in an organisation at a certain level of maturity. We also raise a number of questions we encourage you to answer before making a decision on CAM.



Q: Do you have the right organisational structure, at the governing body and management levels with a commensurate set of roles and responsibilities that are well defined?

The organisation needs to have well defined organisational structures with roles and responsibilities for risk management and control assurance clearly defined. Very often these need to expand beyond the realm of a traditional audit committee and historical management structures as they would need to include control assurances on people matters, financial matters, technical or operational matters, health safety and the environment, technology, stakeholder management, and all the six 'capitals' that King IV and the International Reporting (IR) framework eloquently define as financial, manufactured, intellectual, human, social and relationships and natural capitals.

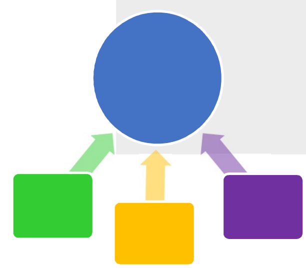
Before a combined assurance model can be considered, there must be a formal understanding of all the stakeholders in an organisation, both internal and external. Organisations' management teams tell us that for the majority of organisations, there are at least 15 or more external assurance activities or providers, ranging from regulator audits to ISO audits to labour, health and safety audits, insurance audits, internal and external audits. Add to this a layer of complexity where different stakeholders provide assurance on the first, second and third lines of defence (LODs) and one starts getting overwhelmed just the very prospect of a CAM.
The ISO 31000:2009 Risk Management Standards also tell us that stakeholder identification (and understanding and communication) is a necessary step in identifying, understanding, and managing its risks. The intellectual, human, social and relationships capitals need to be completely understood, if you have any chance of identifying those stakeholders that are important, necessary and play a role in assurance activities in the first place.
For many organisations, these can include internal or external (traditional) audit service providers, regulators, customers- yes some customers conduct audits – other service providers, banks and financial institutions, forensic service providers, management and those that OWN the risks and their controls in an organisation. In most instances it also means appointing CAM champions within different parts of the organisation or having an increased number of assurance professionals to pull the various streams and stakeholders together.

Q: Do you have a complete stakeholder map, stakeholder strategy and has it been developed in a meaningful fashion for CAM implementation?

Before assurance of controls can take place, you need to know where you are and where you are heading via a clear set of strategic and operational objectives. You then need to know what your risks are and how/when/where they can affect the achievement of where you want to be. You need to know who owns the risks and you also need to know what controls are employed to manage what risks and who owns such controls. Otherwise you can't provide assurance in any meaningful way. In the absence of this information it is near impossible to have clear sight of what the associated controls are that manage these uncertainties, never mind providing value based assurance of such controls.

Q: Do you have a clear set of strategic and operational objectives? Are they risk assessed?

Q: Do you have the risks documented and the controls documented in a way that creates an understanding of the uncertainties facing the achievement (read exceed or fail to achieve) of objectives for the various objectives and their associated uncertainties (read risks) at the different levels of the organisation?

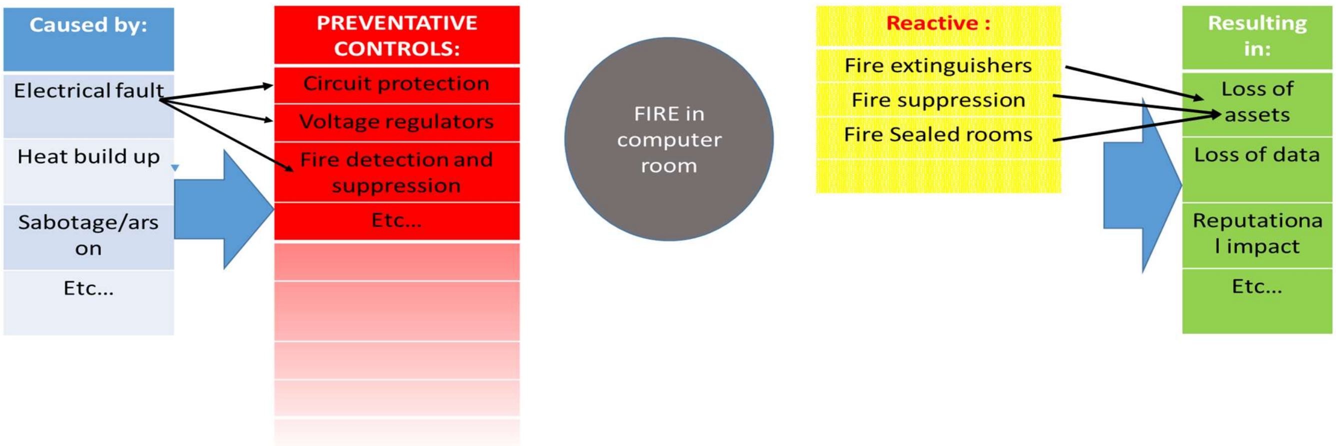


Over years of involvement in many organisations, the variations of assurance reports, languages and definitions used, and processes followed almost matches the number of organisations we've had the privilege of assisting over the years. When looking at the results of an ISO 9000 or 14 000 audit, an integrated reporting audit, a financial audit, an internal control-self assessment audit, a safety or health audit, the list goes on, the reports rarely even look the same. More often than not, they follow disparate audit processes, different languages, and different sets and are reported on in different reporting formats and structures.

Q: Have you set a common language, process, and reporting structure for various assurance activities?

Many organisations believe that for every risk, there should exist a multiplicity of controls to deal with the risk. Has anyone ever really stopped to understand and analyse the controls so that its clear what controls are actually aimed at the cause of the risk and what controls are aimed at the consequence of a risk.

The highly simplistic bow-tie below demonstrates this:



There is still no organisation that we have come across that has the money or the time to be able to get assurance for every control on every risk. In order to apply CAM as a value add proposition to assist and support management, the governing body and its sub-committees, it is therefore important to have enough granularity and understanding of the risk (and its causes) and the preventative controls and reactive controls that are in place so that assurance activities can be focussed on the most important controls (typically but not always preventative). Many organisations have gone beyond risk bow-ties to inform assurance activities and have evolved to have robust and defensible processes to identify KEY controls from the myriad of controls that may exist. Second and third LOD then only become concerned with assurance of the key controls and not all controls.

Q: Do you know your risks; do you understand their root causes? Is it clear what controls are aimed at causes and what controls are only there to reduce the direct consequence, like insurance?

Q: Do you have a defendable process to identify key controls from a myriad of controls?

The answer to our opening question, "should we all aspire to a combined assurance model?", is clearly yes. When to do it and how quickly depends largely on the organisational maturity and especially its risk management maturity and culture. If you can't answer yes confidently to the few questions posed in this paper, rather set to work on being able to answer yes to those questions. Then consider tasking management with the design and implementation of a CAM.

Contact:
Zanorashe Bwakura
zbwakura@mondialcons.com
+27 71 686 0053

Mondial Consultants (PTY) LTD.
www.mondialcons.com
Phone: +27 861 007 662
Fax +27 86 564 0005

Office Address
17 Central Office Park
257 Jean Avenue
Centurion
South Africa