Convergence of ERM & IA In Providing Assurance

Shagen Ganason

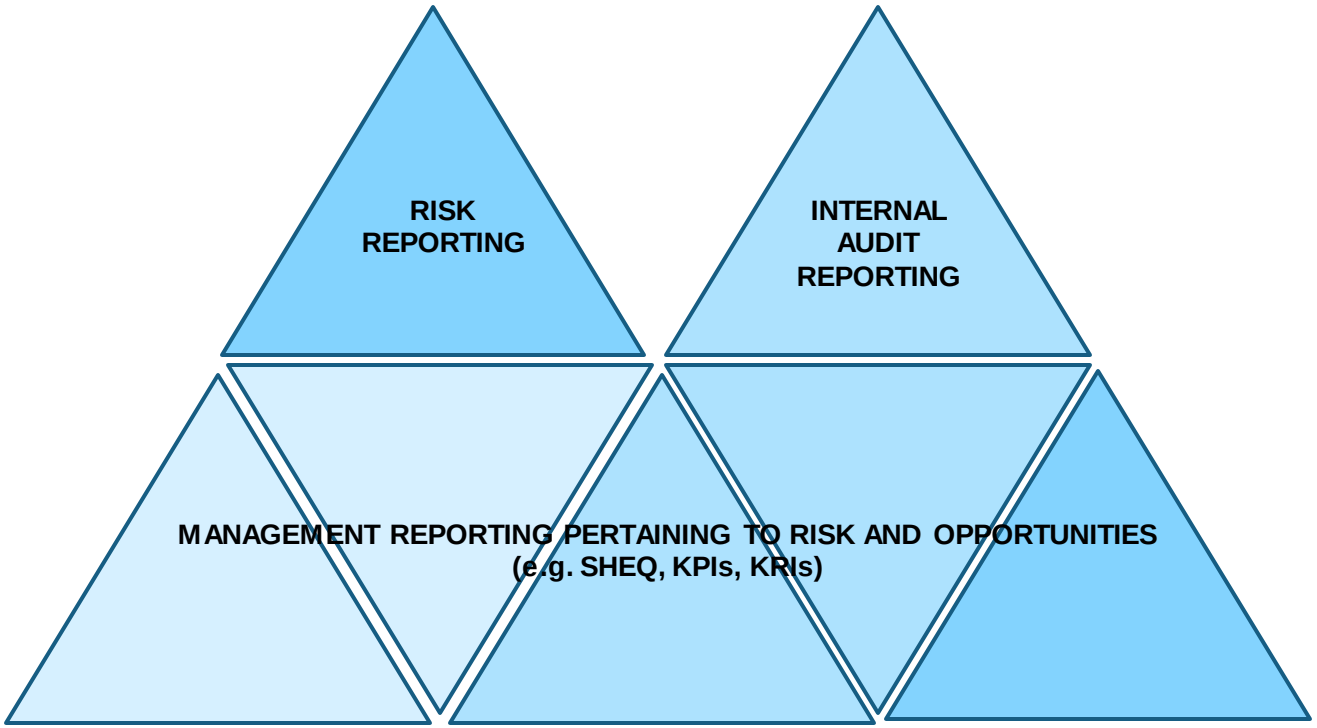
Te Puni Kokiri, New Zealand

20 August 2015

2015 IIA INDONESIA NATIONAL CONFERENCE
IIA INDONESIA Tentrem Hotel, 19 - 20 August 2015 | Jogjakarta, Indonesia

The Institute of Internal Auditors Indonesia

Is this familiar?

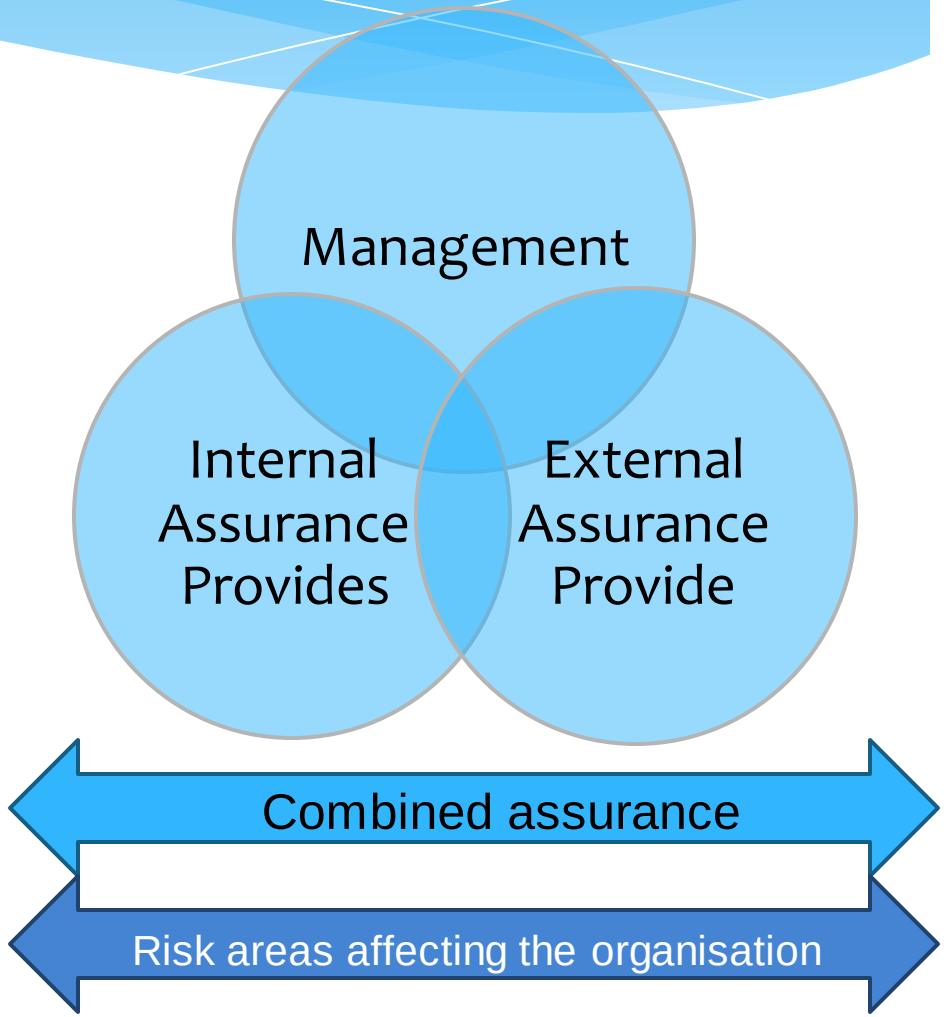


Learning Objectives

* King III on Combined Assurance
* Where is it risky
* Are we focusing on where it matters
* Critical areas of convergence
* Effective cooperaton
* Benefits of combined assurance

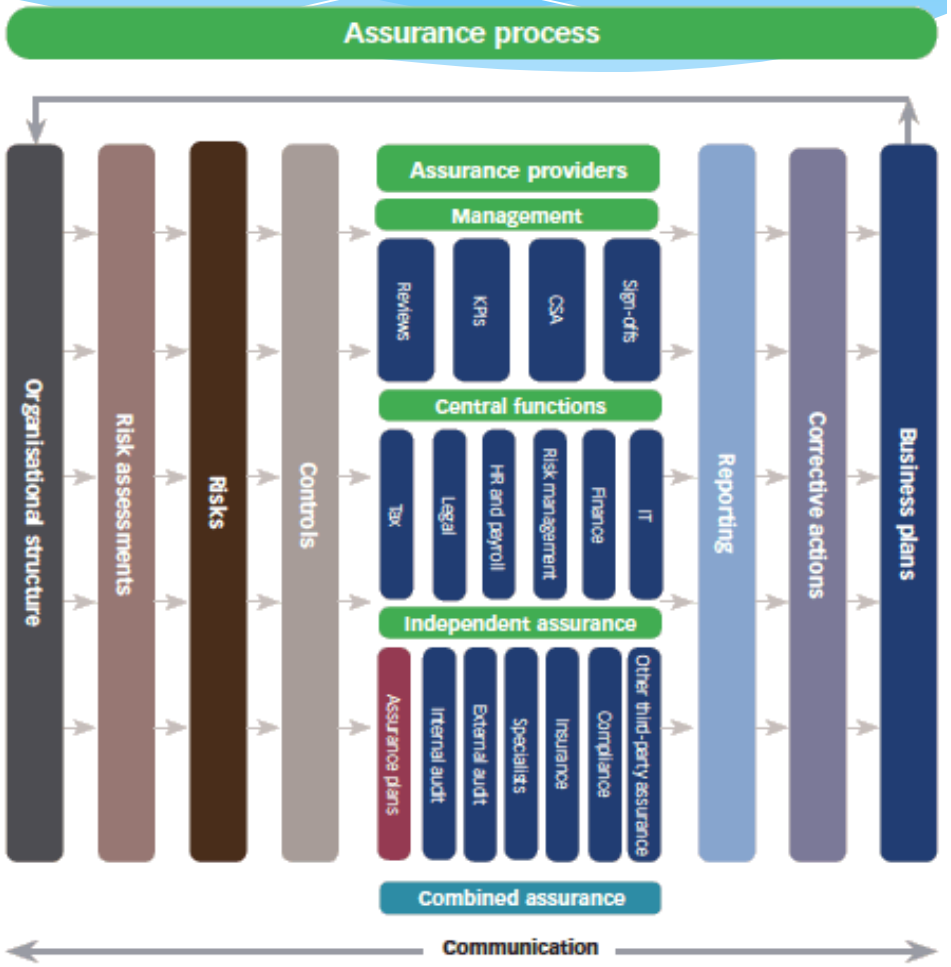
King III Report

3.5 *The **Audit Committee** should ensure that a **combined assurance model** is applied to provide a **coordinated approach** to all assurance services*



Combined assurance

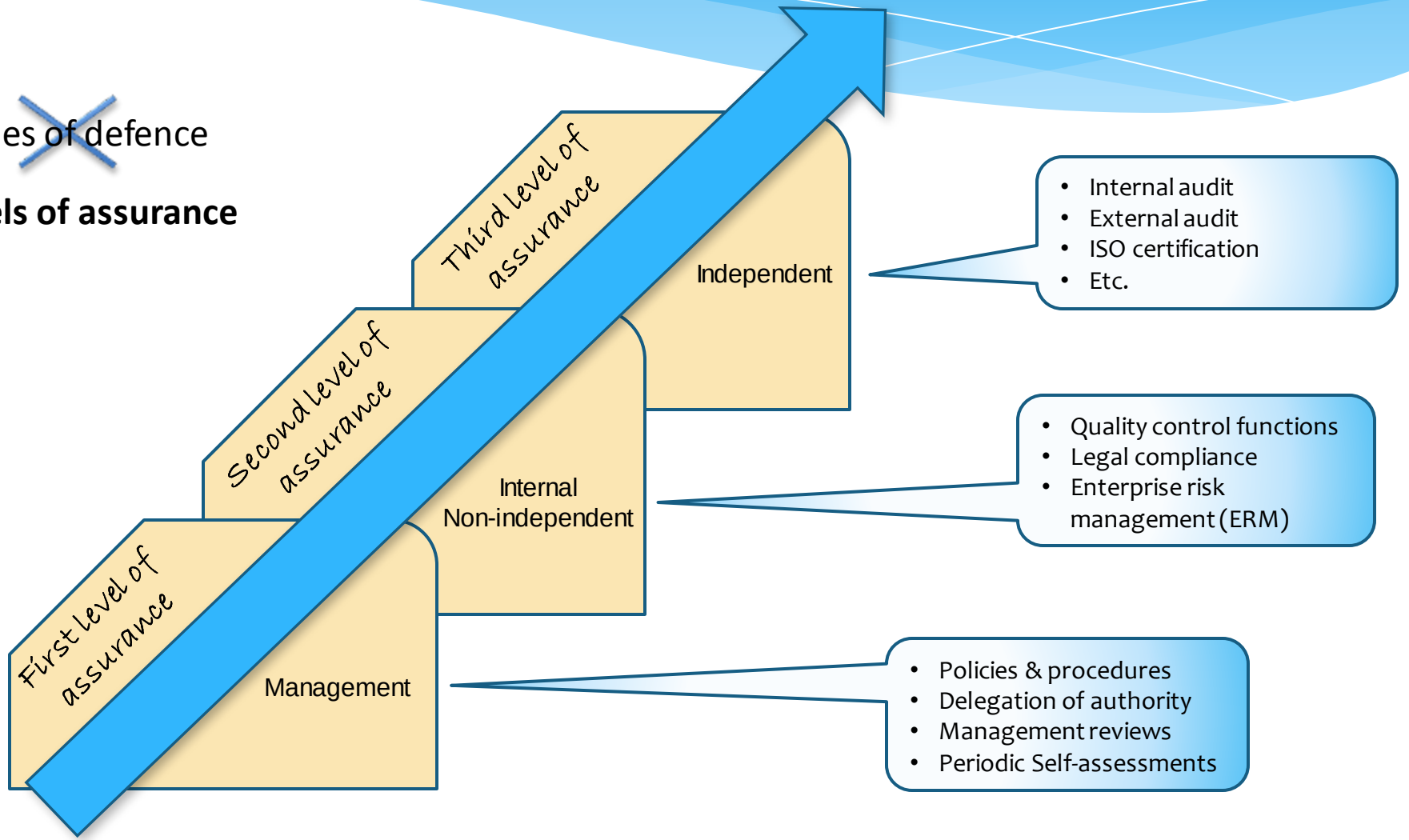
- What is combined assurance?
- Assurance reality check
- Risk mapping
- Combined assurance design



Understanding Assurance

~~3 Lines of defence~~

3 Levels of assurance



King III on risk management and combined assurance

The board should ensure that frameworks and methodologies are implemented to increase the probability of anticipating unpredictable risks

King III on Internal Audit and Combined Assurance

The board should receive assurance regarding the effectiveness of the risk management process

Chief Risk Officer

1	• Provide overall leadership, vision and direction from ERM
2	• Establish an integrated framework for all risks in the organisation
3	• Develop risk management policies including quantification of management's risk appetite
4	• Implement a set of risk indicators and reports including incidents and losses
5	• Communicate the organisation's risk profile to stakeholders
6	• Develop analytical systems and data management capabilities to support the risk management program

Chief Audit Executive

1. Champion risk management across the organisation
2. Evaluate the Enterprise Risk Management methodologies and processes to ensure that they are working as intended
3. Review and provide assurance that the risks of the organisation are being systematically identified, evaluated and appropriately managed
4. Monitor and evaluate the adequacy and effectiveness of the risk mitigation responses designed by management
5. Report to the Audit Committee on the effectiveness of the Enterprise Risk Management process, procedures and internal controls

Can CAE and CRO collaborate?

* What does ERM mean?
* How do both functions fit into the equation?
* How can internal audit assist and yet independently evaluate risk management activities?

Is there convergence between Internal Audit and ERM?

ERM Definitions

RIMS: ERM is a **strategic** business discipline that **supports** achievement of an organization's **objectives** by addressing the **full spectrum of its risks** and managing a **combined impact** of those risks as a interrelated **risk portfolio**

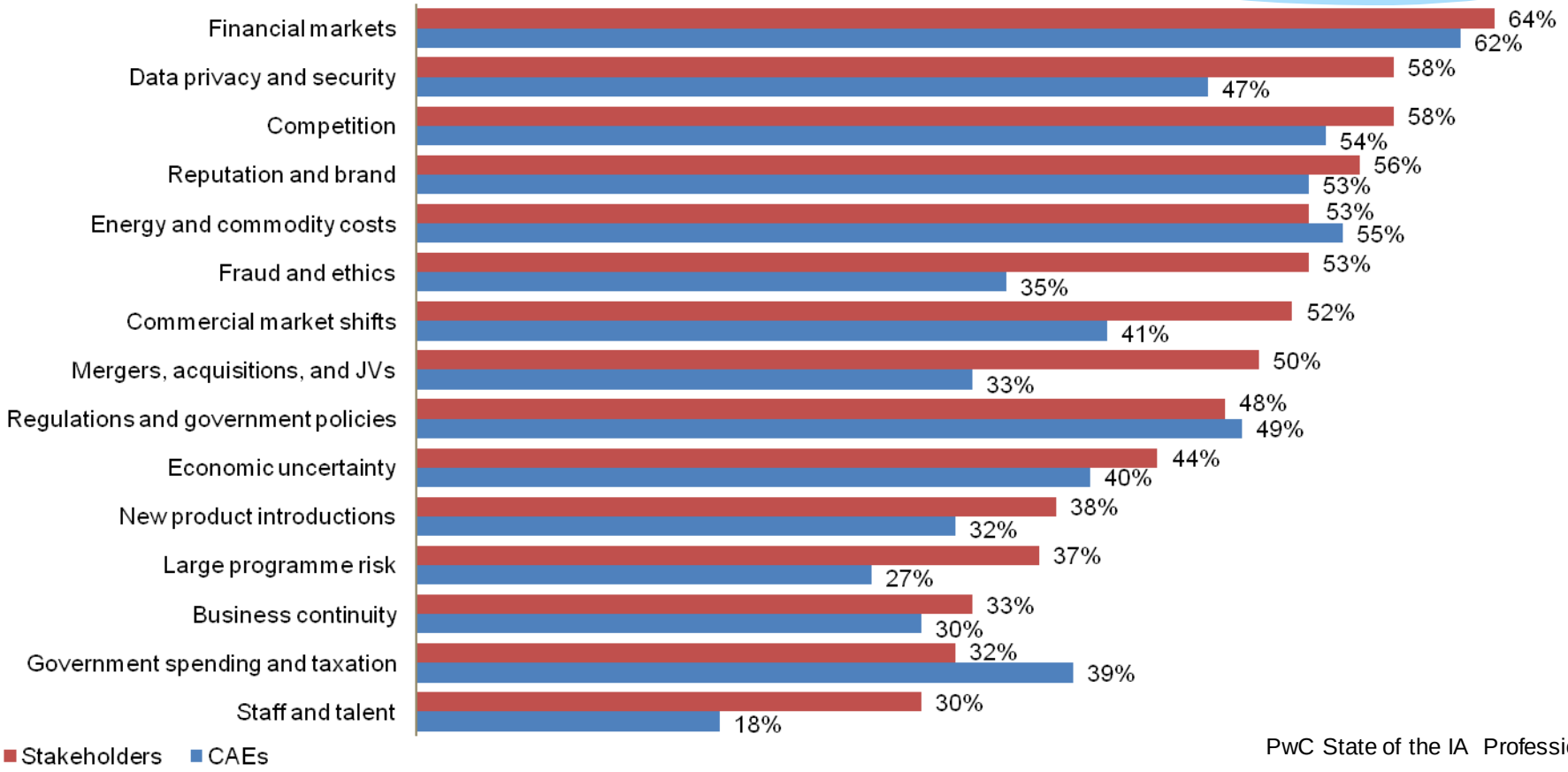
The IIA: ERM is a **structured, consistent and continuous** process across the **whole organization** for identifying, assessing, deciding on responses to and reporting on **opportunities and threats** that affect the achievement of **objectives**.

Source: The IIA and RIMS

Managing risk has to make sense……

Risks that are generally not perceived as well managed

How well is risk being managed?



PwC State of the IA Profession Study

For convergence to work…

* Are risks adequately covered in the risk profile?
* Is risk information simplified or excessively cluttered?
* Is risk information communicated credible?
* Stakeholder consensus on risks raised by management?
* CAE robust dialogue with CRO around ERM?
* Does IA have enough resource?
* **Is ERM effective?**

Results of Ineffective Risk Management

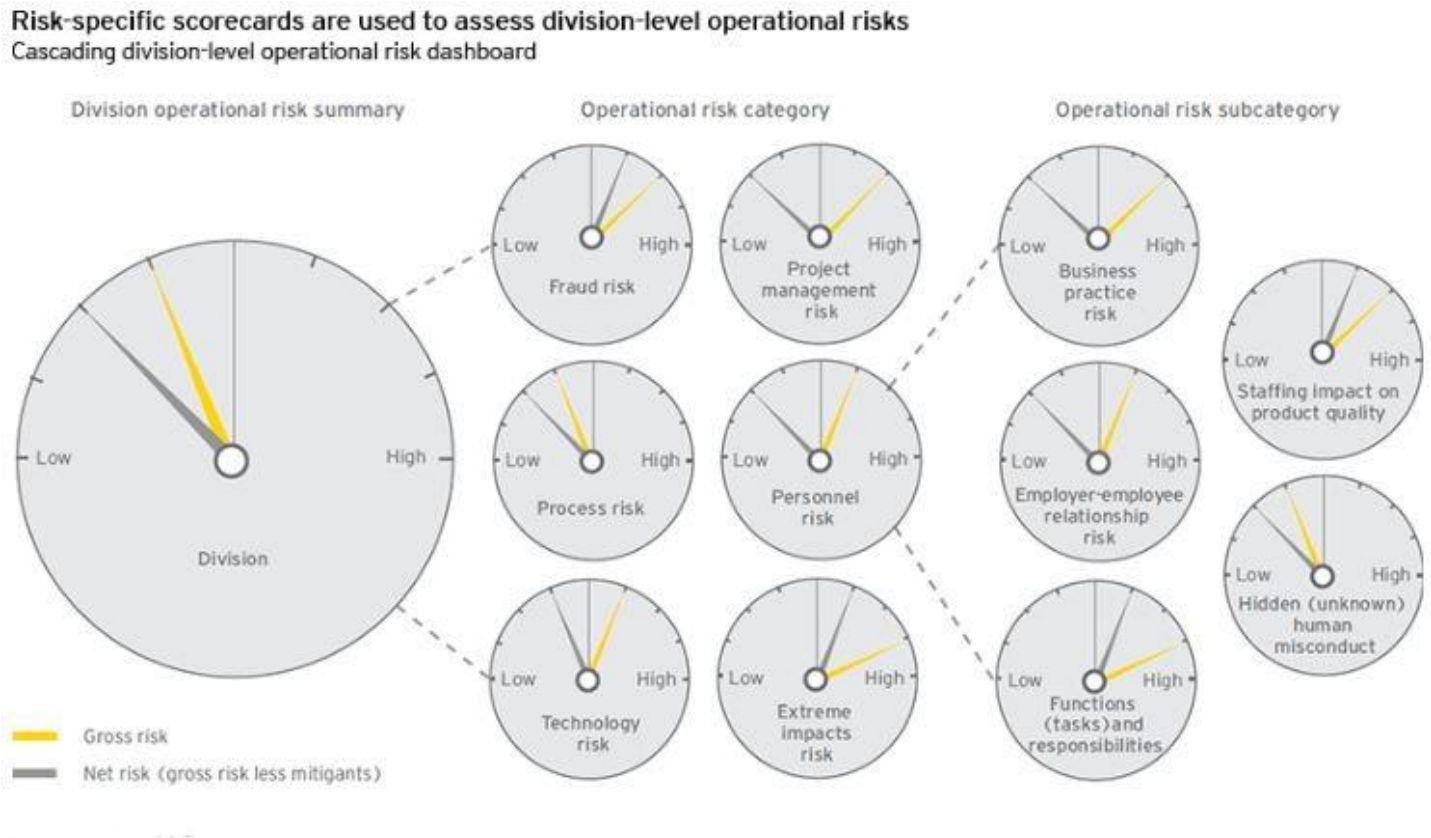
* Poor identification of risks
* Breakdown in internal control that could prevent the organization from achieving its objective
* Reactive responses to potential risks, rather than proactive
* Changing/ new risks are not adequately identified, controlled and managed
* Inability to leverage on internal audit expertise e.g. root cause analysis, impact assessment etc.
* Inability to leverage on ERM expertise

Summary

To ensure successful convergence of ERM and IA :

* A common risk language
* Enabling technology
* Clearly defined roles
* Approved policy to ensure commitment to cooperate
* A communication plan – encompassing ongoing communication/dialogue
* Involvement from senior leadership – “tone at the top”
* Continued coordination, reporting and communication
* Provision of necessary and appropriate training

Combined Risk Scorecard



Questions
Comments