

Combined Assurance : Holistic Assurance approach for Organization

Seminar Nasional Internal Audit
Lombok, 16 April 2014

Fandhy Haristha Siregar,
CIA, CISA, CISM, CISSP, CRMA, QIA, CEH, CEP-PM



Contents

- 3 Lines of Defense
- Assurance Providers
- Why Combined Assurance?
- Combined Assurance Approaches
- What are the Critical Success Factors?
- Combined Assurance: CIMB Niaga Study Case

3 Lines of Defense

First line of defence	Second line of defence	Third line of defence
Management oversight	Management of risk	Independent assurance
Objective: Setting strategy, performance measurement, and establishing and maintaining risk management, control and governance across the	Objective: Providing a risk framework to improve decision making, planning and prioritisation of the business activities.	Objective: Provides independent and objective assurance of the overall adequacy and effectiveness of governance, risk
 <div> <p>Is there any silo approaches and/or competing one another?</p> <p>Is any potential redundancy and/or assurance fatigue within assurance clients?</p> <p>Are they competent enough?</p> <p>Are these effective enough?</p> </div>		
Assurance Providers: Management Quality assurance functions Other: Project Management Office	Assurance Providers: Risk: Risk Management, Regulatory Risk Management, Legal Risk Management, Other: Forensics, Consultancies within the business, e.g. Tax.	Assurance Providers: Internal Audit External Audit/Advisors External regulators

Assurance Providers

There are three fundamental classes of assurance providers:

1. **Those who report to management** or are part of management (management assurance), including individuals who perform control self-assessments, quality auditors, environmental auditors, and other management (designated assurance personnel).
2. **Those who report to the board**, including internal audit.
3. **Those who report to external stakeholders** (financial statement assurance), a role traditionally fulfilled by the independent/statutory auditor.



Why Combined Assurance?

- Optimize the **effectiveness of assurance providers, create a synergy** between assurance providers and avoid assurance fatigue
- To **improve coverage** of the wider audit universe through combined assurance.
- To create confidence in the assurance has been provided **on key/significant risks and to promote efficiency**
- To implement *Standard 2050* of IPPF & King III (South Africa)

What is the **difference** between Combined Assurance & Integrated Assurance?

Combined Assurance Approaches

- Combined assurance integrates & co-ordinates all assurance, by:
 1. Understanding the risks. Aligning assurance to the critical risk exposures;
 2. Understanding who are all the assurance providers;
 3. Realization of what is actually assurance;
 4. Reported within the governance structures;
 5. Coordinating the assurance activities; and
 6. Consolidating the risk and assurance profile.
- Two approaches:
 1. Top-Down
 2. Bottom-up



Combined Assurance Approaches – Top Down



Combined Assurance Approaches – Bottom Up

- Reviews by “offsite” subject matter experts to be conducted during these time windows
- Reviews to be coordinated by Internal Audit
- An experienced leader appointed to manage each departmental review
- Reviews cover system compliance and effectiveness and opportunities
- Review findings are prioritised and ranked
- Review findings are referenced back to the risk register

<gambar bottom up>



Combined Assurance - References

Standard 2050
Coordination

King III

2050 – 1 Coordination

- 1 Organization's assurance provider framework can consist of internal audit, external audit, governance, risk management, or other business control functions

2050 – 2 Assurance Maps

Assurance map is a valuable tool for coordinating risk management and assurance activities.

2050 – 3 Reliance on the Work of Other Assurance

- 3 **Providers** The results of other assurance providers can be integrated with the work of internal audit in a comprehensive opinion to key stakeholders. A good coordination attracts greater reliance on internal audit.

Internal Audit as Catalyst of Combined Assurance

bringing new perspective in Governance, Risk & Control and promote Combined Assurance through establishment of CAR Forum.

Combined assurance should be based on identified risks and how assurance is achieved and reported to the Board / Accounting Authority.

What are the Critical Success Factors of Combined Assurance?



Standards 2050 - Coordination

1



- 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 minimize duplication of efforts.**
- This responsibility requires the CAE's inclusion and participation in the organization's assurance provider framework. This **framework can consist of internal audit, external audit, governance, risk management, or other business control functions/disclosures** performed by the organization's management team.
- Inclusion and participation in this framework helps ensure that the CAE is aware of the organization's risks and controls in relation to organizational goals and objectives.
- Boards will use various sources to gain reliable assurance, including management, internal audit, and third parties.



Practice Advisory 2050 – 1 Coordination

- Oversight of the work of external auditors, including coordination with the internal audit activity is the responsibility of **The Board**
- Coordination of internal and external audit work is the responsibility of **The Chief Audit Executive**
- The CAE obtains the support of the board to coordinate audit work effectively.
- The external auditors may rely on the work of the Internal Audit Activity in performing their work.
- Planned audit activities of internal and external auditors need to be discussed to ensure that **audit coverage is coordinated and duplicate efforts are minimized where possible.**
- These assist external auditors in determining and adjusting the scope and timing of their work.
- On the other hand, external auditors presentation materials and management letters need to be understood by the CAE and used as **input to internal auditors in planning the areas to emphasize in future internal audit work.**



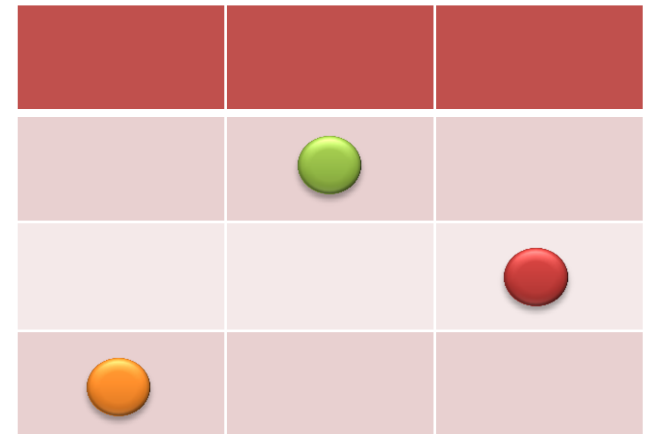
Practice Advisory 2050 – 2 Assurance Maps

- Increased focus on the roles and responsibilities of senior management and the Board has prompted many organizations to place a greater emphasis on **assurance activities**.
- This guidance addresses **how the Board is responsible for ensuring that business-critical risks are being assured and adequately managed**.
- An “assurance map” is an organizational tool that will **prevent redundancy**, as well as some areas falling through the cracks.



Practice Advisory 2050 – 2 Assurance Maps

- The Standards defines Assurance as “an objective examination of evidence for the purpose of providing an independent assessment on governance, risk management, and control (GRC).
- Assurance Map provides:
 - Who is doing what,
 - What has been done to date,
 - Provides comfort to those at the top that all participant are being responsible and accountable
- Steps of creating Assurance Mapping:
 - Step 1: Establishing the business case
 - **Step 2: Assurance reality check (what risk, source of assurance, how)**
 - **Step 3: Risk mapping**
 - **Step 4: Combined assurance design**
 - Step 5: Implement



Assurance Reality Check

- Identify Assurance Provider (Internal Audit, Risk Management, Compliance, Information Security, SOX Compliance, Quality Assurance)
- Competency Assessment of Assurance Provider:
 - Skill & Experience levels
 - Scope & frequency of work
 - Acceptable approach/methodology
 - Conflict of Interest
 - Number of staffs
 - Quality review



Risk Mapping with ERM Fundamentals

- Risk naming conventions
- Shared understanding of risk and control information
- Proper risk description
- Agreement on residual risk exposure and target (desired) risk rating
- Understanding if controls really mitigate risk exposure
- Does the information on incidents feed back to the risk register



2.3



Sample of Risk Mapping

2.3

Example IT risk	Associated controls	Three lines of defence assurance providers								
		First line of defence - Management			Second line of defence – Risk and legal based assurance			Third line of defence – Independent assurance		
		Control self assess	Mgt review	Special project	ERM	SOX	Compliance	External audit	Internal audit	Special project
Operational - Network										
Network perimeter security breach	Secure firewall configuration		✓		✓	✗				✗
	Secure remote access design	✗	✓						✓	
	Security monitoring service contracted with supplier	✓	✓			✓		✓	✓	
Network downtime	Service level agreement with supplier	✓	✓			✓		✓	✓	
	Disaster recovery plan	✓	✓		✗	✓			✓	

Currently providing assurance

Should provide assurance

✓ Quality of assurance acceptable




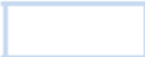
✗ Quality of assurance unacceptable

Scope excludes detailed configuration

Sample of Assurance Mapping & Reporting

2.4

Processes	Three lines of defence assurance providers								
	First line of defence - Management			Second line of defence – Risk and legal based assurance			Third line of defence – Independent assurance		
	Control self assess	Mgt review	Special project	ERM	SOX	Compliance	External audit	Internal audit	Special project
Strategic									
Funding	Moderate	Extensive	Not applicable	Moderate	Extensive	Not applicable	Not applicable	Inadequate	Moderate
Sustainability	Extensive	Extensive	Extensive	Moderate	Moderate	Inadequate	Extensive	Extensive	Not applicable
Growth	Extensive	Extensive	Extensive	Moderate	Inadequate	Not applicable	Inadequate	Extensive	Inadequate
Operational									
Treasury	Inadequate	Moderate	Not applicable	Inadequate	Extensive	Extensive	Extensive	Inadequate	Inadequate
Products and services	Inadequate	Moderate	Not applicable	Inadequate	Extensive	Not applicable	Extensive	Moderate	Extensive
Finance	Inadequate	Moderate	Extensive	Moderate	Extensive	Not applicable	Extensive	Moderate	Inadequate

 Extensive assurance
  Moderate assurance
  Inadequate assurance
  Not applicable

Source: IIA Conference 2012: Risking It Combining It, Jhetam, Bilal

Sample of Assurance Mapping & Reporting

Example of ranking of assurance

Rating	Description/Characteristics guidance
Extensive Assurance	<ul style="list-style-type: none">• Scope of work covers entire process area• Period of the work performed covers more than half the year• Positive opinion or certification is provided• Accredited assurance provider
Moderate Assurance	<ul style="list-style-type: none">• Scope of work covers part of the business process• Work performed covers less than 6 months of the period under review• Limited assurance statement provided
Limited Assurance	<ul style="list-style-type: none">• Scope of work covers a very specific part of the business process• Work performed is for a period less than 3 months or is at a point in time• No certification or assurance statement provided (e.g. factual findings with recommendations)

2.4

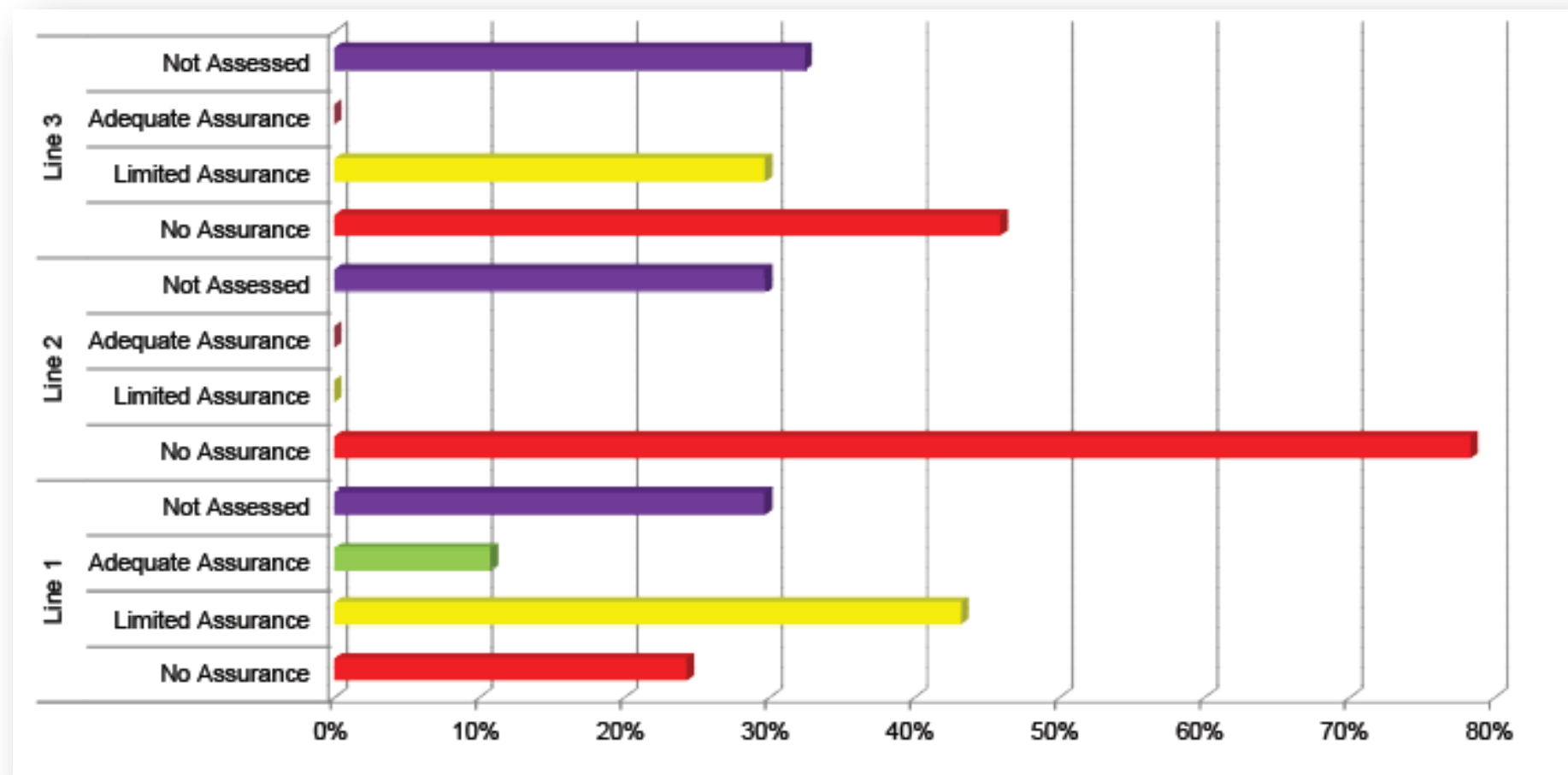


Sample of Assurance Mapping & Reporting

Risk No	Risks	Line 1				Line 2						Line 3			
		Control Self Assessment		Management Review		IRM		Compliance & Regulatory		Legal		Internal Audit		External Audit/ Other	
		Actual	Proposed	Actual	Proposed	Actual	Proposed	Actual	Proposed	Actual	Proposed	Actual	Proposed	Actual	Proposed
1	ABC is unable to control minimise reputational damage during crises and unable to restore reputation due to non approval of communication strategies	Not applicable													
2	Uninformed, de-motivated workforce caused by lack of relevant and timely communication	Not applicable						Not applicable							
3	Not meeting the milestones for new organisational design	Not applicable													
4	Equipment theft & vandalism							Not applicable							
5	Energy theft							Not applicable							
6	Inability to collect all our revenue														
7	Inadequate Engineering Definition During Project Planning and Development														
8	Delays In Acquiring Servitudes	Not applicable													
9	Investment decision delays	Not applicable						Not applicable		Not applicable				Not applicable	
10	Primary Energy Challenges														
11	Shareholder support	Not applicable						Not applicable							
12	Loan - Inadequate revenue to service Investec Loan	Not applicable						Not applicable							

Not assessed
 No assurance
 Limited assurance
 Adequate assurance

Sample of Assurance Mapping & Reporting (cont'd)



■ Not assessed
 ■ No assurance
 ■ Limited assurance
 ■ Adequate assurance



Source: PwC Combined Assurance Practical Approach

Sample of Assurance Mapping & Reporting (cont'd)

Ref No	Risk description	Mitigating actions (existing or planned)	Accountable	Responsible	Line 1	Line 2	Line 3	Assurance Provider	Nature of Assurance	To whom reported	Management Assessment	Comment
6	Legislation and regulatory changes and uncertainty threaten the sustainability of ABC	Maintain marketing position of quality fuels: Increase availability on the forecourts.	GM: Sales & Marketing	Legal and Compliance officer	a	a		Line 1: Manager	Line 1: Monitor sales on a monthly basis (Niech product sales vs. Lead replacement product sales) with a report.	Line 1: GM level & Mancom	Room for improvement	Infrastructure not available.
								Line 2: Business support	Line 2: Prepares reports	Line 2: GM level & Mancom		

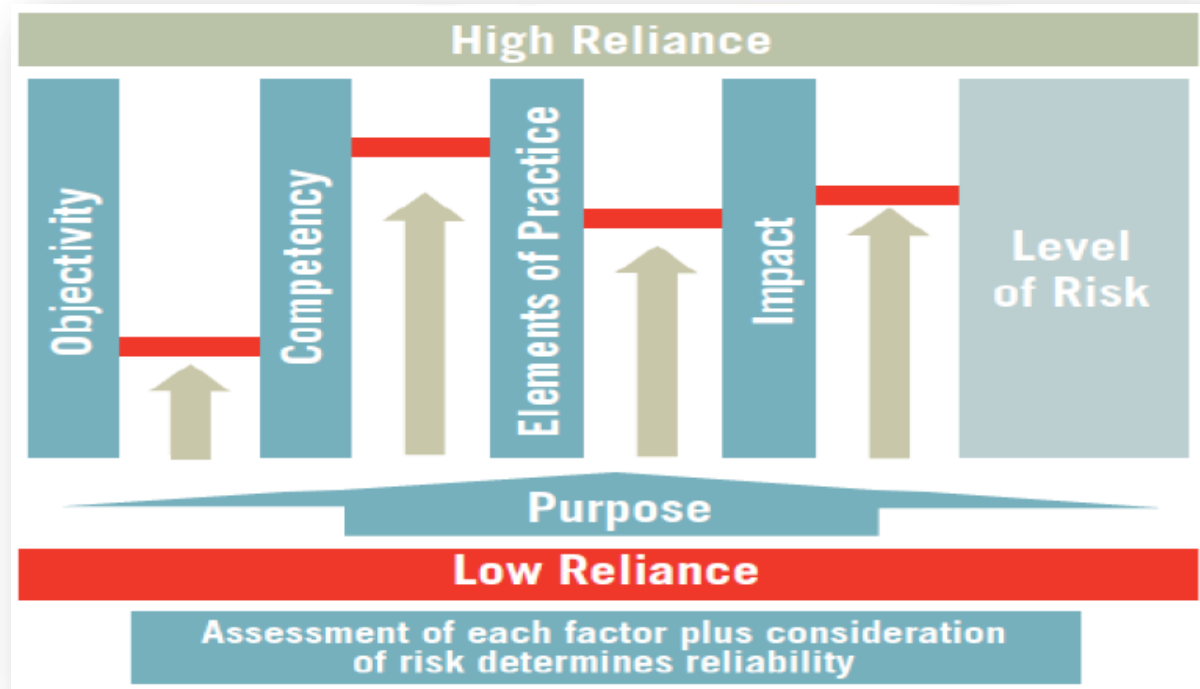
2.4



Practice Advisory 2050 – 3 Reliance on the Work of Other Assurance Providers

Five Principles in Determining Reliance:

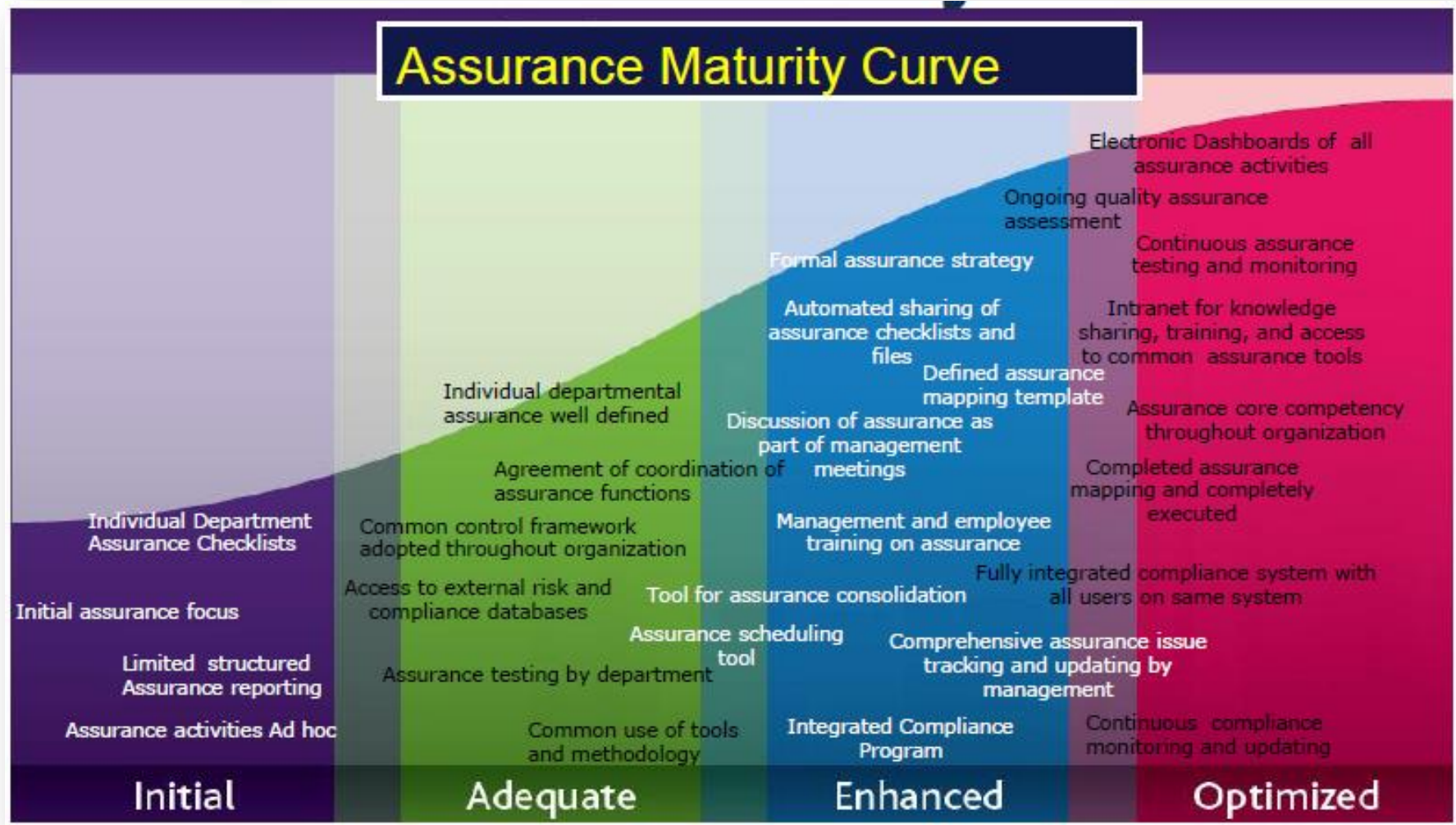
1. Purpose
2. Independence and Objectivity
3. Competence
4. Elements of Practice
5. Communication of Results & Impactful Remediation



Source: IPPF of IIA, Practice Guide Reliance by Internal Audit on Other Assurance Providers, Dec 2011

Assurance Maturity Model

3



Source: IIA International Conference 2012, Anderson, Urton., Assurance Mapping, 2012

Internal Audit Roles in Combined Assurance

- IA assisted in coordinating the initial development of consolidated risk assurance maps
- Together with Risk Management, IA coordinated with Business and Support units in validating the consolidated assurance maps
- Review the application and effectiveness of Combined Assurance practice:
 - Assess the quality of assurance
 - Assessment of the adequacy of Combined Reporting (combined assurance reporting)



Risk Maturity : At which Risk Maturity Level ?

Partnership concept

Risk Maturity	Key Characteristics	Internal Audit Approach
Traditional	No formal approach developed for risk management	Promote risk management and rely on audit risk assessment
Awareness	Scattered silo based approach to risk management	Promote enterprise-wide approach to risk mgt and rely on audit risk assessment
Defined	Strategy and policies in place and communicated. Risk appetite defined.	Facilitate risk management/liaise with risk management and use management assessment of risk where appropriate.
Managed	Enterprise wide approach to risk management developed and communicated.	Audit risk management processes and use management assessment of risk as appropriate.
Integrated	Risk management and internal control fully embedded into the operations.	Audit risk management processes and use management assessment of risk as appropriate.

Source: The Institute of Internal Auditors

Combined Assurance “CIMB Niaga Case Study”



The Black Hole of Assurance



- The economic crisis provides evidence that boards of directors operate in **a partial assurance vacuum**, whereby boards rely on their top executive teams to provide the assurance, but too often that **assurance is partial and insufficiently objective**.
- Filling the board's assurance vacuum (black hole) will **require a change in internal auditing paradigm, positioning, and reporting method**.
- Future CAEs, while remaining independent of the board, will **need to have equal status with executive directors** so that they can interface on equal terms and attend board meetings as well as some board committee meetings.

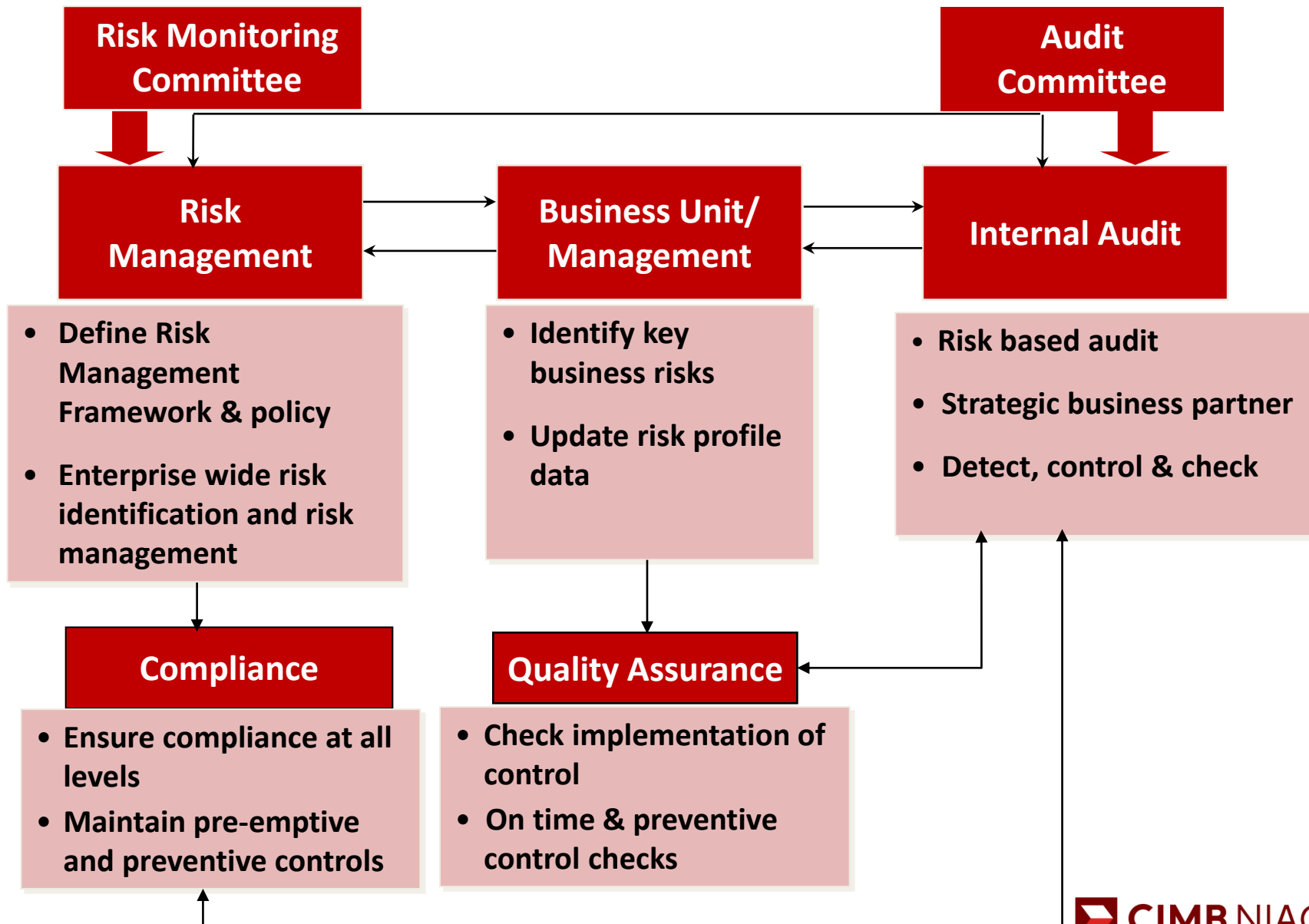


CIMB Niaga Chief Audit Executive is part of Board of Management, and actively being involved in several High Level Committee with regards to Governance, Risk, Compliance

Internal auditors
ent criteria
judgment.
within their

respective organizations will help provide stronger assurance to the board.

Coordination of Compliance, Audit & Risk Management



Make Combined Assurance a Reality

- Executive sponsor, audit committee support and management commitment
- Combined Assurance Champion, driving day-to-day activities:
 - Needs to be driven actively
 - Consistent reporting structure and feedback
 - Regular assessment of quality of delivery
- Combined Assurance Forum (3 – 6 monthly assessment)
- Common Risk Language and Alignment
- Convince all stakeholders of future approach, create combined assurance blue print (assurance and risk mapping, combined assurance reporting and continuous improvement)
- Centralized libraries to ensure consistency and data integrity

Internal Audit can lead this process !



Milestones & Achievements

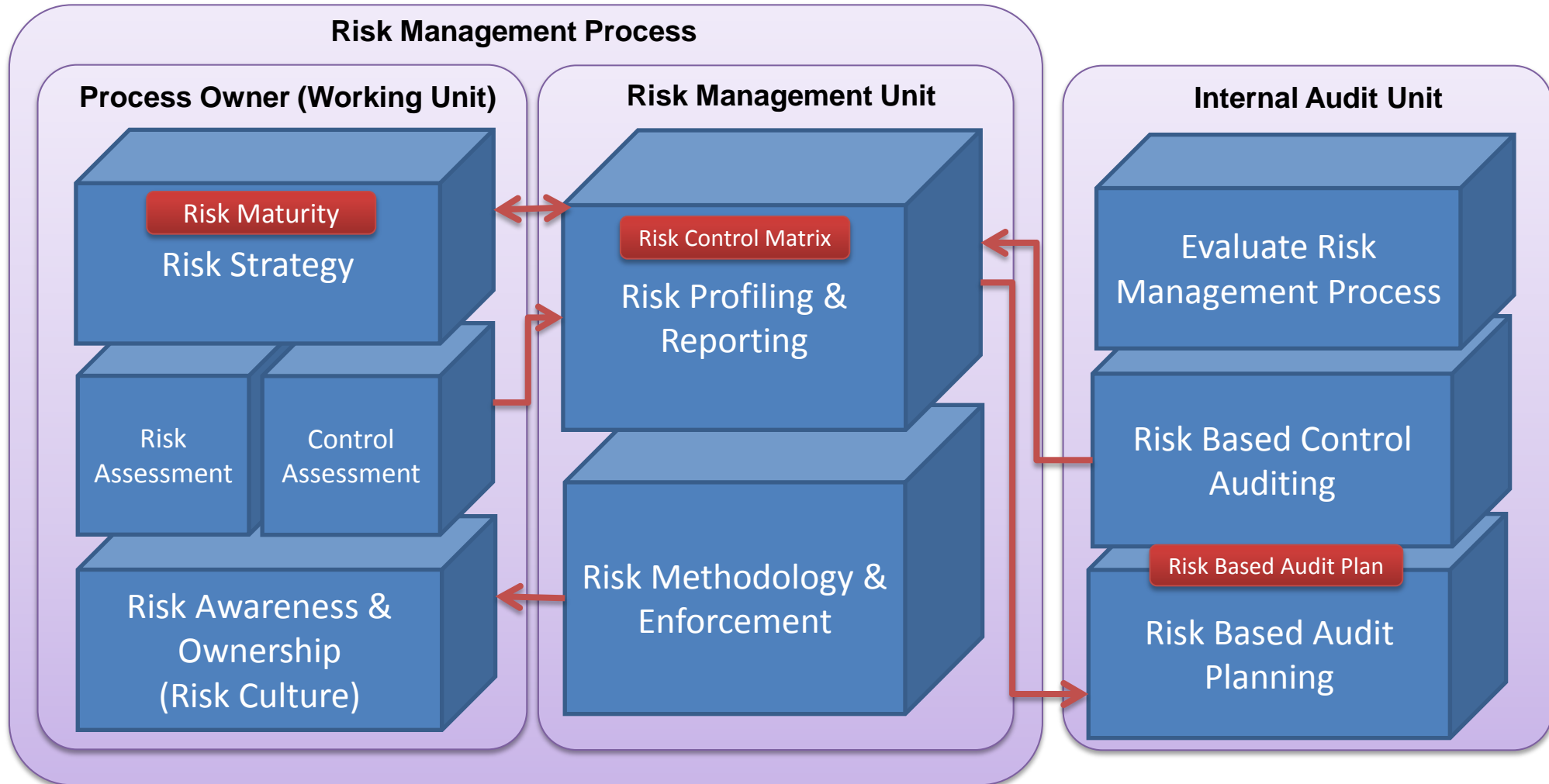
Done

- Established Compliance-Audit-Risk (CAR) Forum:
 - Local Compliance-Audit-Risk Forum – Monthly
 - Regional Compliance-Audit-Risk Forum – Annually
- Role sharing between assurance providers has been discussed and formulated with regards to significant products & activities (facilitated by Group Internal Audit and Group Risk Management)

Strategic Initiatives

- Work in progress (could be facilitated by Internal Audit):
 - Formal Assurance Mapping between assurance providers
 - Centralized Risk & Control Library across the assurance providers

Aligned & Centralized Risk-Control Database across Assurance Providers



Thank You