Evolution of Internal Audit and Risk Management in Central Banks – Interaction between the lines of defence

IMF/Hawkamah
Central Bank Governance Forum
Dubai, December 2014

Agenda

- The importance of good governance in central banks post the global financial crisis
- The evolution, role and nature of Internal Audit in Central Banks
- The evolution, role and nature of Risk Management in Central Banks
- The relationship and interaction between IA and ERM
- Combined Assurance to those charged with Governance of Central Banks
- Practical considerations – The SARB experience
- Conclusion: The importance of adding value
The importance of good governance in central banks post the global financial crisis

Global developments influencing governance and risk management in central banks

- Volatile, uncertain, unpredictable environment
  - Global financial crisis and recession – challenges for central banks
  - Recent global geopolitical events/natural disasters
  - Policy makers need to be able to focus on core tasks knowing ERM is effective

- Increased emphasis on governance and transparency
  - Governance failures
  - Critically important for central banks – expanding role, complexity and risk
  - Require appropriate structures, policies, framework and approach

- More explicit financial stability mandate
  - Increased external focus on independence, accountability and governance
Developments in corporate governance

- King Report and Code on Corporate Governance (third version) contain recommended principles for corporate governance in SA
- Chapter 4 (of 9) devoted to the Governance of Risk
- The SARB strives to apply the principles of King III, to the extent deemed appropriate for a central bank

King III, Chapter 4 - The Governance of Risk

- Board responsible for the governance of risk
- Board determines the levels of risk tolerance
- Risk/audit committee assists board with risk responsibilities
- Board delegates to management the responsibility to design, implement and monitor a risk management plan
- Board ensures risk assessments performed on a continual basis
- Board ensures frameworks/methodologies implemented to anticipate unpredictable risks
- Board ensures management considers/implements appropriate risk responses
- Board ensures continual risk monitoring by management
- Board receives assurance regarding the effectiveness of the risk management process
- Board ensures processes in place for complete, timely, relevant, accurate and accessible risk disclosure to stakeholders
Risk management in central banks

- Not simply based on institutional risk and return considerations
- Takes into account national interest, statutory and constitutional responsibilities
- Central banks function within an environment of continuous change and uncertainty
- Monitoring and analysis of, and appropriate responses to, potential/actual risks from global political & economic environment are critically important

Risk management in central banks (contd)

Central banks are largely risk-averse institutions -
- disruption to operations or damage to reputation could seriously jeopardise satisfactory fulfilment of roles and responsibilities
- executive management of central banks are intensely aware of the high performance standards that all stakeholders expect

A strong integrated risk management function viewed as an integral part of good corporate governance:
- to help the Board carry out its governance oversight role; and
- to help management focus on the challenges attendant to primary goals
The evolution, role and nature of Internal Audit in Central Banks

The evolution of internal audit approaches

- Inspection of operations against standard operating procedures. Seen as “policing” function.
- Globalisation, governance failures, Treadway commission and COSO
- Rise of Modern Internal Auditing – business partnering, adding value
- Focus on adherence to widely accepted standards, guidelines and best practice
- Quality Assurance, and benchmarking against other organisations
- Professional certification and membership of IIA
- Auditor of the future – continuous auditing, etc.
The role of Internal Audit

- Independent and objective assurance and consulting function to evaluate and improve governance, risk management and control processes
  - Characterised by use of systematic and disciplined approach
- Assurance: Objective assessment of evidence to provide an independent opinion on the adequacy and effectiveness of operations, processes and systems
  - Nature & scope of assurance engagements determined by IA itself
- Consulting: Advisory services performed at the request of management
  - Must maintain objectivity and not assume operational responsibility

IA, in collaboration with others, plays a key role in ensuring a sound control environment that supports effective and efficient achievement of organisational objectives

The key characteristics of Internal Audit

- The key characteristics of IA are independence and objectivity:
  - Independence means: Free from any conditions that limit IA’s ability to be unbiased, impartial and without any conflict of interest
  - Objectivity means: A state of mind that allows auditors to apply pure and principled judgement on audit matters without compromising on quality in subordination to any other views
- These require that IA is well positioned and adequately resourced

Threats to independence and objectivity must be managed at several levels: individual auditor, project, IA function and organisational.
Maintaining independence and objectivity

- Clearly defined and approved Mandate and Charter
- Appropriate structural positioning and reporting lines
- Top-down commitment and support
- Escalation authority and exercising thereof
- International best practice methodology and standards adherence
- Adequate resources – personnel, financial, technical, personality of CAE
- Objective frame of mind
- Research, benchmarking, development, continuous improvement
- Internal awareness creation and marketing
- Quality and credibility

Mandate and Charter of Internal Audit

- Key components of the IA Charter:
  - Purpose, mandate and mission
  - Scope of work – no restrictions
  - Accountability – to Executive management and AudCom
  - Independence – direct escalation access to AudCom
  - Responsibility – plan, execute, develop, report, investigate
  - Authority – unrestricted access, adequate resources, but no operational duties
Other key success factors for IA

- Appropriate composition of the AudCom
- CAE and staff certified professionally and knowledgeable about the organisation and its strategic objectives
- An AudCom approved, risk-based audit plan fully aligned with the strategic and operating objectives of the organisation
- Making use of technology and modern, automated and continuous auditing techniques
- Accurate, lucid, thematic and relevant audit reporting to management and AudCom
- Demonstrable AudCom backing on sensitive findings and matters
- Periodic external Quality Assurance Reviews to promote credibility

Successful IADs focus on the most significant risk exposures – those that preclude the organisation from achieving its most critical strategic objectives.

The evolution, role and nature of Risk Management in Central Banks
Risks faced by central banks
(Core functions)

- Failure to provide credible economic information to effectively support economic policy formulation
- Ineffective implementation of monetary policy
- Failure of the settlement system
- Inadequate or ineffective regulation and bank supervision
- Inability or failure to identify actual threats and vulnerabilities to financial system stability
- Failure to ensure the availability of a secure national currency
- Ineffective administration of the exchange control system
- Ineffective management of the official foreign reserves

Risks faced by central banks
(Support structure and systems)

- Failure to maintain an adequate, competent and effective work force
- Failure of critical ICT systems
- A lack of or ineffective business continuity capability
- Inadequate, ineffective, inefficient or uneconomical properties, physical infrastructure, office space and corporate support services
- Ineffective legislation, invalid agreements, incorrect legal advice and opinions
Risks faced by central banks (consequential risks)

- Exposure to specific financial risk elements, as a consequence of foreign reserve management and market operations
- Failure to adequately secure the Bank’s cash holdings and large value payments
- Possible litigation due to failure to adhere to contractual obligations or fulfilment of duties in terms of relevant legislation, including the SARB Act
- Poor financial discipline, excessive expenditure and failure to accurately effect payments and process transactions

Risks faced by central banks (reputational risk)

Reputational risk -

- is probably one of the biggest consequential risks that the Bank is faced with, which means that if the other categories of risk are not properly managed, the Bank’s reputation could suffer substantial damage
- is closely linked to the conduct of and communication by, especially, the executive management of the Bank
- can arise even when all other risks are managed effectively by the Bank, when there is a mismatch between public perceptions and the actual objectives, actions and resources of the Bank
Risks faced by central banks (exogenous risks)

- Significant changes in prices of traded goods/services
- Significant changes in the macroeconomic policy and/or practices of Government
- Significant negative socio-economic developments and/or megatrends
- Global, regional or local political unrest or geo-strategic developments
- Significant global or regional financial shocks or instability
- Significant global slow-down in economic growth or a global recession
- External security risks - criminal activity, cash heists, cyber crime, counterfeiting of notes and coin, money laundering, as well as activist and terrorist activity
- Disruptions to or failure of services such as electricity, water and telecommunication

The role of a centralised ERM function

- To establish, promote, coordinate and monitor the governance of risk management practices and processes through standardised policy, framework, structures and methodologies throughout the organisation
- Help management at all levels ensure:
  - that no risk events occur that could threaten the achievement of business objectives.
  - achievement of business objectives in an effective, efficient (cost and time) and timely manner.
The role of a centralised ERM function (contd.)

- Facilitate maintenance and implementation of a Risk Management Policy and organisation-wide common approach to dynamic risk management at all levels
- Provide a standardised approach, methodology and tools for risk management
- Promote RM awareness and provide RM training and support to management at all levels
- Facilitate and monitor systematic risk identification and mitigation action plans
- Ensure standardised and integrated reporting of diverse risk information to management and governance structures
- Provide specialist support for technical cross-cutting risks, e.g. business continuity, information security.

Key characteristics of ERM

- It is an extension of management, providing a centralised service
- It does not take ownership of Risk Management away from any level of management, it merely centralises coordination and monitoring of the “how” of risk management
- It administers an organisation-wide forum of risk coordinators who cooperate to help manage diverse types of risk through harmonised processes
- It facilitates risk identification, evaluation and reporting, and monitors mitigating activities for residual risks
- It maintains the central repository of risk related information of the organisation
- It ensures relevant risk information from diverse operations are reported to governance structures in clear, comprehensive, concise, accurate and relevant form
- It provides assurance to the governance structures (Risk Management Committee (RMC) and Board Risk Committee (BRC))
Other key success factors for ERM

- Top-down commitment and support for the Risk Management Policy of the organisation
- Adherence to international frameworks/standards for risk management, such as COSO ERM or ISO 31000
- Systematic approach and methodology to ensure comprehensive identification of all risks to the organisation
- Facilitation of integration of strategy, risk management and performance management
- Successful inculcation of a risk intelligent culture throughout the organisation, where risk management is second nature and part of everyday decision-making
- Facilitation of and contribution to combined assurance to the Board Risk Committee

ERM trends and activities in central banks

- Transitioning from operational risk focus to strategic and policy risks
- Developing universal repositories of actual risk event information
- Fostering risk awareness/risk culture
- Linking different operational risk disciplines
- Improving risk incident management and information
- Enhancing risk reporting
- Improving use of automated tools

IORWG Surveys 2011 - 2013
# The relationship and interaction between IA and ERM

## IA and ERM: Comparative table

<table>
<thead>
<tr>
<th></th>
<th>IA</th>
<th>ERM</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Positioning</strong></td>
<td>Independent from management</td>
<td>Extension of management</td>
</tr>
<tr>
<td><strong>Standards</strong></td>
<td>Well developed</td>
<td>Developing</td>
</tr>
<tr>
<td><strong>Resources</strong></td>
<td>Professionally certified</td>
<td>Certifications emerging</td>
</tr>
<tr>
<td><strong>Mandate and scope</strong></td>
<td>Assessment of controls, unrestricted scope but no operational responsibilities</td>
<td>Standardisation, facilitation, coordination, monitoring</td>
</tr>
<tr>
<td><strong>Added value ability</strong></td>
<td>Dependent on culture</td>
<td>Achievable with sound approach</td>
</tr>
</tbody>
</table>
The relationship between IA and ERM

- A sound, co-operative working relationship is needed between Enterprise Risk Management (ERM) and Internal Audit (IA)
- Regular interaction and communication is critical
- The combined assurance model can form the basis for co-ordinated planning and monitoring of work of both parties
- Cross-membership of governance committees should be considered, i.e. the CAE could be an *ex officio* member of the Risk Management Committee and the CRO could attend AudCom meetings

The relationship between IA and ERM

- Results of risk assessments should be shared with IA
- These results should be considered by IA during its risk based planning processes – both holistic (annual) planning and planning for individual audits
- Relevant IA working papers should also be shared with ERM to inform and aid operational risk assessment processes (to avoid duplication and improve efficiency)
- Audit findings should be shared with ERM to inform the risk assessment process and, where applicable, update the risk incident register
- IA should avoid turning known risk information into audit findings
Combined Assurance to those charged with Governance of Central Banks

King III defines Combined Assurance (CA) as “integrating, coordinating and aligning the risk management and assurance process within an organisation to optimise and maximise the level of risk, governance and control oversight over the organisation’s risk landscape”

- CA improves coverage and quality of assurance provided to those charged with governance by better understanding, planning and coordinating work of all assurance providers
- CA helps to identify any assurance gaps in key areas and avoids overlapping of assurance effort that could result from assurance providers working in isolation
Combined assurance (contd)

- Combined assurance is about:
  
  Ensuring the right amount of assurance, according to the risk tolerance of the organisation, in the right areas, from people with the best and most relevant skills, as cost effectively as possible, in order to obtain the trust of those charged with governance in the organisation.

- Assurance coverage is optimised by coordinating the three levels of defence against any risk:
  
  - Management control,
  - Integrated risk management, and
  - Independent assurance providers.

The three levels of defence

- Management - First line of defence against any risk comprises essential management functions such as preventative and detective controls design, on-going management review, control self-assessments, performance management and special initiatives to identify and combat specific risks in particular technical areas and circumstances.

- Enterprise risk management - Second line of defence is best achieved by a targeted organisation-wide approach to risk management. It comprises elements such as departmental risk identification and mitigation, centralised risk management facilitation using uniform approved policies, risk measurements, tolerances, approaches, methodologies, specialised risks (e.g. information security, business continuity, health and safety, fraud) and compliance monitoring and reporting.

- Independent Assurance - Third line of defence comprises internal audit, external audit, and other credible external assurance providers such as technical consultants and control experts in special circumstances. Internal audit is by charter and structural design wholly independent from management, and therefore offers a high level of assurance.
Fundamentals for combined assurance

- Combined Assurance Forum with terms of reference
- Agreement by all role players on the structure of the combined assurance model
- Agreement on residual risk exposure and desired risk ratings
- Common understanding of whether or not controls actually mitigate risk exposures (adequacy of controls)
- Information on incidents must feed back to the risk register and be taken into consideration
- Understanding of and adherence to ISA 610 by External Auditors

Combined Assurance Model

- The main principle of the approach is that assurance coverage is optimised by considering the three levels of defence: Management, Enterprise Risk Management and Independent Assurance
- The Model is used to plan the various assurance activities to be performed, including assigning responsibilities
- The Model is also used by the CAF (and oversight committees) to monitor the execution of the plan
- The results of assurance work performed are populated in the Model and the information is used to compile a report on combined assurance
Benefits of combined assurance

- Supports co-ordinated and relevant assurance, focusing on key risk exposures
- Ensures improved reporting to the Board and its sub-committees
- Facilitates comprehensive coverage and prioritised approach in monitoring remedial actions to improve identified weaknesses
- Provides support for audit committees in making statements in annual reports relating to the reliability of financial statements
- Breaks down silos, ensures more comprehensive assurance
- Promotes efficiency through joint advance planning and coordination
- Globally there is a move towards stronger assurance structures
- Both internal and external audit support comprehensive combined assurance models

Practical considerations – The SARB experience
IAD Governance

- The IAD is governed by an **Internal Audit Charter**
- IAD reports to both the Governor and the Audit Committee
- IAD activities are guided by the International Professional Practices Framework (IPPF) of the IIA
- The relationships with our clients are guided by protocols/service level agreements that address the following:
  - Audit planning
  - Audit process
  - Reporting process
  - Follow-up process on implementation of management action plan to resolve control deficiencies
  - Handling of disputes

Assessment of the IAD

**External to the department:**
- Quarterly Assessment of the department
- Annual Audit Committee Assessment
- Quality Assurance Review by IIA

**Internal to the department:**
- Internal Quality Assurance and Improvement Programme
- Staff evaluations per project, quarterly and annually
- Assessment of CIA annually by Governor
Risk management policy

- Largely based on the principles contained in the COSO ERM Framework
- Consistent with widely accepted standards, guidelines and best practice
- Benchmarked against other central banks
- Membership of IORWG - International Operational Risk Working Group for central banks

Risk management policy (contd)

Definition of risk
- Risk is defined as any factor, internal or external to the Bank, that could have a negative impact on or prevent the achievement of valid/relevant organisational objectives, as well as the pursuit of irrelevant or invalid organisational objectives

Four broad risk categories are defined in the policy
- strategic risk
- financial risk
- operational risk
- reputational risk
What works well?

- Executive & Board commitment and support for creation of framework for full integration from the start
- Integrated approach provides proper basis for comprehensive risk reporting and enhancing understanding of business – gives cross-functional and integrated perspective
- Top-down, phased approach ensures 80% gains in 20% of total implementation timeframe
- Framework provides practical and effective mechanism for identification of key risks across the Group
- Clear work programme for oversight committees
Pitfalls and challenges

- Attempting to achieve too much in too little time – apply phased approach, emphasise quality rather than quantity
- Awareness creation and understanding by all “hub-and-spoke” role players takes considerable time and effort
- Difficult to determine appropriate levels and ensure a consistent level of assessment across the risk universe
- Remains a challenge to determine/anticipate and respond to Board and executive needs & requirements
- Co-ordinating ERM is a complex and demanding task – ensure sound relations and cooperation with role players

Some future challenges

- Integrating strategy, risk management and performance management
- Integrated reporting, and providing assurance on non-financial content of annual reports, i.e. sustainability and social contribution
- Researching frameworks for assessing and measuring policy risks
- Finding a single risk measure for central banks (a proxy for RARORAC)
- Fixing central banks’ capital structures to reflect the risk exposure
Conclusion: The importance of adding value

Generic top of mind issues include:
- New Legislation, Regulation
- Global economic conditions, market access, growth, expansion into Africa
- Sustainability, innovation, new technologies, energy supply/costs, social responsibility
- Environmental change, calamity risk, BCM
- Leadership, talent management
- Collaboration, partnerships, M+A
- Economic policy, nationalisation, infrastructure, labour unrest, E/R volatility.

Is IA reporting focused in these issues? Does ERM help to ensure that risk intelligence permeates management decision-making regarding such issues, as opposed to being an afterthought?
### Frequent questions for IA and ERM

- Where was IA/ERM, why was this not picked up before?
- We are tired of IA/ERM, do you have to audit/risk-assess us again?
- Why does it look as if you are duplicating each other?
- What do you know about our specialist operations - why go beyond just the financial controls?
- What is this IA Report/Risk Matrix telling me?
- What value does this report add?

Instead, questions should be:

- We are concerned about an aspect of our operations, please assess our risks and controls. Can you help find out what went wrong here? How can we make sure something similar does not happen again?

### What could IA do to add more value?

- Ensure staff have the right understanding of the organisation’s business and operations to competently assess its critical processes
- Develop an audit plan that covers a high proportion of the organisation’s high risk business units and operations
- Be alert to new and emerging trends and risks to the organisation and adapt the audit plan accordingly
- Audit as many as possible of the high-risk business units and processes continuously using automated techniques
- Do frequent skills audits and external QA reviews against IIA Standards
- Pre-empt typical questions asked by Boards
**What should ERM do to help?**

- Position ERM correctly in the organisation – balance between extension of management, vs. useful assurance provider in combined assurance approach
- Understand the business objectives and management's needs
- Facilitate integration of Strategy, Risk Management and Performance Management
- Increase risk adeptness of management and governance structures
- Assist in Board induction and ongoing development and effectiveness
- Make risk mitigation activities targeted, focused, effective
- Adapt, and help management and the organisation adapt, to changing circumstances/requirements, e.g. Integrated/sustainability reporting

**What could both IA and ERM do to add more value?**

- Communicate effectively - identify common themes, consolidate, synthesise, present concisely
- Give expert advice, not volumes of detailed data. Provide solutions to problems, not information about problems
- Know when to stand on principle and when to compromise
- Build and cherish credibility. Judge on facts, not rumours or inside information, verify everything, be discreet, keep confidentiality.