CONVERGENCE OF GOVERNANCE : RISK : COMPLIANCE

Presented by:
ANN GATONYE
Cert ERM

THURSDAY, 06TH JULY 2017
CONVERGENCE

What is it?
Outline of the session

✧ Definition of GRC
  • Risk
  • Compliance
  • Governance

✧ Evolving Risk Management & Compliance

✧ Convergence of GRC
Governance, Risk and Compliance (GRC) refers to Organisation’s co-ordinated strategy for managing the broad issues of:

Corporate Governance

Enterprise Risks Management

And

Corporate Compliance
Governance

The effective, ethical management of a company by its executives and managements levels
Governance

 Cadillac • Provide guidance on sound and proactive corporate governance
 • Consider corporate governance as one element for consumer protection
 • Determine whether the organisations have adopted and effectively implemented sound corporate governance policies and practices
 • Assess the quality of organisation’s audits and control functions
 • Evaluate the organisation’s group structure
 • Bring to the board and management’s attention on problems they detect through their supervisory effort
Risk Management

The ability to effectively and cost-efficiently mitigate risks that can hinder an organisation’s operations or ability to remain competitive in its market.
Compliance

The Organisation’s conformance with Regulatory requirements for business operations, data retention and other business practices
THE EVOLVING RISK MANAGEMENT !!!
# Risk Management

## Physical & Financial Assets

<table>
<thead>
<tr>
<th>Focus</th>
<th>Financial and hazard risks and internal controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Objective</td>
<td>Protect Enterprise value</td>
</tr>
<tr>
<td>Scope</td>
<td>Treasury, Insurance and operations primarily responsible</td>
</tr>
<tr>
<td>Emphasis</td>
<td>Finance and operations</td>
</tr>
<tr>
<td>Application</td>
<td>Selected risk areas, units and processes</td>
</tr>
</tbody>
</table>
# Business Risk Management

Physical, Financial, Customer, Employee/suppliers Assets

<table>
<thead>
<tr>
<th>Focus</th>
<th>Business risk, internal controls taking risk by risk approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Objective</td>
<td>Protect Enterprise value</td>
</tr>
<tr>
<td>Scope</td>
<td>Business managers accountable</td>
</tr>
<tr>
<td>Emphasis</td>
<td>Management</td>
</tr>
<tr>
<td>Application</td>
<td>Selected risk areas, units and processes</td>
</tr>
</tbody>
</table>
# Enterprise Risk Management

Physical, Financial, Customer, Employee/Supplies and Organisational Assets

<table>
<thead>
<tr>
<th>Focus</th>
<th>Business risk, internal controls taking an entity-level portfolio view at risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Objective</td>
<td>Protect and Enhance Enterprise value</td>
</tr>
<tr>
<td>Scope</td>
<td>Apply across the enterprise, at every level and unit</td>
</tr>
<tr>
<td>Emphasis</td>
<td>Strategy setting</td>
</tr>
<tr>
<td>Application</td>
<td>Enterprise-wide to all sources of value</td>
</tr>
</tbody>
</table>
Business/Strategic Risk arises as much from the likelihood that something good will not happen as it does from the threat that something bad will happen.

Risk management is not risk avoidance – it is maximizing the risk/return relationship – it is about taking risks knowingly not unwittingly.

Risk can be defined as the combination of the probability of an event and its consequences (ISO/IEC Guide 73).

Remember...

You cannot eliminate all risk
Risk-taking is an inherent element of a business and, indeed, profits are in part the reward for successful risk taking. On the other hand, excessive, poorly managed risk can lead to losses and thus endanger the safety of a business.
Traditional

- Process is fragmented
- Risk is viewed as negative
- Reactive and ad hoc behaviour is acceptable
- Transaction based – cost based
- Narrowly focused and functionally driven
- A reporting centre
Integrated approach

- Risk is viewed as positive and that successful organisations must take risks to seize on opportunities
- Proactive behavior is expected
- Risk management is strategic – value based
- Broadly focused and process driven
Bretton woods and its impact
- Officially implements in Dec 1945
- It established a system of fixed FX rates around the US dollars
- A bi-product was a framework of fixed interest rates
- Organisations had framework providing certainty

In the 1960s it came under increasing pressure
- Moved to a system of quasi-floating FX rates and collapsed in Feb 1973 with uncontrolled FX

Faced uncertainty, customers turned to banks for assistance
- This resulted into growth in off-balance sheet, unregulated derivatives. The uptake was minimal but it grew very rapidly

By early 1980s, regulators realised that they were losing control, and in 1985 bank of England and Fed Reserve of New yorl published a paper recommending;
- Introduction of banking regulation
- Formation of the foundation for the first Basel Accord in 1988
First Accord

The regulatory scene before;
• No international consistency of regulation
• Uniform, ignoring individual risk profiles based on size of business
• Only on-BS activities regulated, typically through liquidity constraints

Objectives of the first accord
• Increase capital ratios
• Harmonise capital requirements (across G-10)
• Include on and off balance sheet

Initially only considered Credit risk (all except debt/equity trading positions)

Subsequently Market Risk Amendment was introduced in 1996, covering trading exposures

The accord was deemed to be broadly successful – banks capital was significantly raised across the global sector
Internal models were introduced (Static Framework - black box)

1991, the first draft of market risk amendment was published but the banks had been developing more sophisticated market risks methodologies (VaR – value at Risk)

1995, the Basel committee agreed that the bank could develop and use own methodologies
1) For internal purpose
2) For them estimating regulatory capital

As a result, the bank-supervisory relationship changed

Supervisors had to understand and to validate the individual models

***the supervisory skills had to change
Business space

In the meantime there were well-publicised end-user losses;

- Bankers Trust
- Merrill Lynch
- Daiwa NY
- Showa Shell Sekiyu
- Metal/gesells Chaft

All this are pre-Baring bank losse US$1billion
And
The public perception of banks become extremely negative and this lead to

G30 report: where the following key areas were discussed;

- Senior management responsibilities
- Systems and control
- Product valuation and approvals
- Adequate disclosure
New Basel Accord

Extension of the objectives

- To maintain at least the current level of capital
- To enhance competitive equality
- To contain probabilistic approached to capital adequacy that are appropriately sensitive to the degree of risk involved in a bank’s position and activities
- To emphasize on the responsibility of the directors and senior management
- To focus in the internationally active banks

- Consultations keep on taking place and every other period there is a publication

- Basel I, Basel II, Basel III

- Every review has an impact to the capital adequacy, Liquidity which is linked to Risk management
## Basic Structure of the New Accord

<table>
<thead>
<tr>
<th>Pillar 1: Minimum Capital</th>
<th>Pillar 2: Supervisory review</th>
<th>Pillar 3: Market Disciplines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Market Risk</td>
<td>Production of ICAAP Review processes</td>
<td>Available Risk Capital Levels of Risk</td>
</tr>
<tr>
<td>Credit Risk</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operational risk</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Regulatory models for each class of risk</td>
<td>Expected and unexpected losses (Economic Capital – Equity plus retained P &amp;L) Regulatory – Equity plus subordinated debt</td>
<td>Market disclosures Concerns</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Disclosure overload</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enforceability in some jurisdiction</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Timeliness</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Auditability</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cost</td>
</tr>
</tbody>
</table>
Return, Risk and Capital are linked

Whenever you undertake a transaction;

- You expose the organization to risk
- Hence you require capital to cover this risk
- You must ensure an adequate Return on this Capital
- Otherwise, you destroy value

Risk management has evolved;

From the reactive reporting of risk to proactive pricing of risk
GRM Encompasses

Aligning risk appetite and strategy – Management considers the entity’s risk appetite in evaluating strategic alternatives, setting related objectives, and developing mechanisms to manage related risks.

Enhancing risk response decisions – Enterprise risk management provides the rigor to identify and select among alternative risk responses – risk avoidance, reduction, sharing, and acceptance.

Reducing operational surprises and losses – Entities gain enhanced capability to identify potential events and establish responses, reducing surprises and associated costs or losses.

Identifying and managing multiple and cross-enterprise risks – Every enterprise faces a myriad of risks affecting different parts of the organization, and enterprise risk management facilitates effective response to the interrelated impacts, and integrated responses to multiple risks.

Seizing opportunities – By considering a full range of potential events, management is positioned to identify and proactively realize opportunities.

Improving deployment of capital – Obtaining robust risk information allows management to effectively assess overall capital needs and enhance capital allocation.
The Importance of GRC

>*</b> Underlying principles:

➢ Every entity, whether for-profit or not, exists to realize value for its stakeholders.
➢ Value is created, preserved, or eroded by management decisions in all activities, from setting strategy to operating the enterprise day-to-day.

➢ ERM supports value creation by enabling management to:

➢ Deal effectively with potential future events that create uncertainty.
➢ Respond in a manner that reduces the likelihood of downside outcomes and increases the upside.
➢ The management of risk is an integral component of effective Corporate Governance
➢ Promoting proactive management rather than reactive with the early identification and prioritisation of key risks
## Roles within the group

<table>
<thead>
<tr>
<th>GROUP</th>
<th>GROUP BUSINESS</th>
<th>COUNTRY</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk Type or Policy Owners</strong></td>
<td><strong>Group Business &amp; Functional Owners</strong></td>
<td><strong>Legal</strong></td>
</tr>
</tbody>
</table>
| - Set & maintain Group standards & policies  
- Design and implement RMF | - Customise Group & develop business specific policies and procedures | - Provide advice on local regulatory requirements  
- Perform assurance review |
| **Compliance & Risk Type Owners** | **Business & Functional Owners** | **Country Risk Coordinator** |
| - Perform assurance review | - Oversee compliance with policies & standards | - Prepare Country Risk Profile  
- Engage risk management at country level |
| **Board Risk Committee** | **Business Risk Committee** | **Country Risk Group** |
| - Review Group Risk Profile & monitor resolution of significant risks | - Review Risk Profile across the business globally & monitor resolution of significant risks. | - Resolve & monitor strategic Risk issues & trends at country level  
- Review country Risk Profile |
| **Business Line Management/URM/RP** | **Line Management/URM/RP** | **Business Risk Group** |
| - Resolve, monitor risk issues & trends at business level  
- Review business Risk Profile | - Manage day-to-day risks  
- Ensure compliance with policies & regulations  
- Identify & report risks, losses & exceptions | - Resolve, monitor risk issues & trends at business level  
- Review business Risk Profile |

**GOVERNANCE**

**POLICY & STANDARDS IMPLEMENTATION**

**ASSURANCE**
Defining GRC

There are various definitions for GRC, but we shall look into Open Compliance and Ethics group (OCEG), the GRC Capability Model, Red Book, 2.0.

✧ It's a system of people, processes and Technology that enables an organisation to:

- Understand and prioritise stakeholder’s expectations
- Set business objectives that are congruent with values and risks
- Achieve objectives while optimising risk profile and protecting value
- Operated within legal, contractual, internal, social and ethical boundaries
- Provide relevant, reliable and timely information to appropriate stakeholders
- Enable the measurement of the performance and effectiveness of the system while optimising
The Integrated Framework

Risk Governance

- Risk Appetite
- Actions
- Measurement and reporting

1st Line
- 1st Line

2nd Line
- 2nd Line

3rd line of Assurance

Systems
- Governance committees
- Risk domains
- Identification
- Assessment
- Mitigation and control
- Monitoring

Board/Group
- [B/GRC]
- [RTO]
- [GKGS]

Business Function
- [FRC]
- [FRO]
- [BKCS]

Country
- [CRC]
- [CRO]
- [LRKCS]

Business / Support unit
- [BRC]
- [BRO]
- [DOI]

Organisation Structure

Control Assurance
Success factors for Effective GRC

1) Commitment from the top - active commitment, oversight and support from Board and top management

2) Communication

3) Culture –
   - culture of risk awareness
   - One risk language
   - single risk rating methodology for all risks and issues

4) Governance and organization Structure.
   - Sound risk governance
   - Embedding risk managers within individual business lines leads to greater understanding and awareness of risk, and of its link to Performance.
   - Clear connections to strategic and business objectives
   - Risk management tied to incentives (Balanced Scorecard)

5) Information Technology (IT) - Integrated system to support a central repository of risk information-

6) Training and developing people to ensure depth of risk knowledge and skills

7) Adequate Policies, Procedures and Limits

8) Quality and utility of data (MIS) – risk data gathered should be accurate and useful

9) Adequate Internal Controls
Global Focus

✪ Basel Committee
  ➢ Regulatory capital requirements (Basic Indicator and standard Indicators)
  ➢ Supervisory oversight (adequacy)
  ➢ Market discipline (qualitative and quantitative disclosures)

✪ King Committee
  ➢ Corporate Governance
  ➢ Responsibility of Risk management
  ➢ Control Environment
Reflection!

What is our (Kenya, East Africa, Africa) Position?
Reflection!
Reflection!

Video clip
ASANTE SANA !!!