Implementing Enterprise Risk Management

September 2016
What is ERM?

- A process
- implemented by management
- to optimize its risks
- to maximize achievement of its objectives.
What is ERM?

Enterprise Risk Management (ERM) is defined by the Committee of Sponsoring Organizations (COSO) as:

“a process, effected by an entity’s board of directors, management and other personnel, applied in strategy-setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.”

Sharon Holi, HoD Enterprise Risk, Safaricom Limited
A Framework for Risk Management

Governance structure
- Risk Management Philosophy + Risk Appetite
- Oversight
- Values, ethics
- Human Capital-Skills, experience, training
- Delegation of authority

Internal:
- Infrastructure
- Personnel
- Process
- Technology

External:
- Political
- Economic
- Social
- Technological
- Environmental

Strategic Plan, Business Plan, Budgets

Techniques
- Qualitative + Quantitative
- Likelihood + Impact
- Linkage between risks – Portfolio View

Avoidance
Reduction
Sharing
Acceptance

Policies and Procedures
- Operational Review and Audit
- Approval framework
- Reporting
- Verification and reconciliations
- Segregation of duties

Internal and External
- Formal and Informal
- Communication Methods
- Accurate, Timely, Relevant
- Share learning and insight

Monitoring
- Ongoing, continuous process
- Self-Assessments
- Independent monitoring and evaluation
- Adapt to changes
- Improve practices
- Align with best practice

Source: Enterprise Risk Management — Integrated Framework,
Committee of Sponsoring Organizations of the Treadway Commission.
ISO 31000

Defines Risk management principles as well as providing a framework/model
Why implement ERM?

• To achieve corporate objectives more efficiently and effectively?

• [https://www.youtube.com/watch?v=r1g8A--D4I0](https://www.youtube.com/watch?v=r1g8A--D4I0)
What do we need to get right?

Ya... we ended up shutting down our risk management project - there was too much at stake and we were afraid we'd get it wrong.
Pre-requisite of Effective ERM

Risk Management Governance
- Awareness
- Philosophy
- Tolerance/Appetite
- Organization
- Policy

Risk Management Infrastructure
- Methodology
- Tools
- Procedures

Risk Management Process
- Identification & Assessment
- Control Activities
- Risk Mitigation Action Plan
- Monitoring & Reporting
- Information & Communication

Road Map to Effective ERM Implementation
- ISO 31000
- AS/NZS 4360
- COSO ERM
- API
- Basel II

Risk Management Maturity Assessment
- Awareness
- Skills
- Culture
- Image
- Processes
- Confidence
- Resources
- Application

Sharon Holi, HoD Enterprise Risk, Safaricom Limited
Pre-requisite of Effective ERM
Risk Management Governance

TONES AT THE TOP

• Awareness
• Philosophy
• Tolerance/Appetite
• Organisation
• Policy
Awareness and Philosophy

Proactive management
Versus
Wait and see

“What if we don’t change at all ... and something magical just happens?”

Sharon Holi, HoD Enterprise Risk, Safaricom Limited
Risk appetite & tolerance

• The ERM framework introduced the concepts of risk appetite and tolerance.

• Risk appetite is the broad-based amount of risk an entity is willing to accept in pursuit of its mission/vision.

• Risk tolerance is the acceptable level of variation in performance relative to achievement of objectives.

• In setting risk tolerance levels, management considers the relative importance of the related objectives and aligns risk tolerance with risk appetite.

<table>
<thead>
<tr>
<th>RISK RATING</th>
<th>RISK TOLERANCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>We are not sufficiently prepared and immediate action is required</td>
</tr>
<tr>
<td>B</td>
<td>We believe Safaricom can or should do more.</td>
</tr>
<tr>
<td>A</td>
<td>We don't believe Safaricom can or should do more</td>
</tr>
</tbody>
</table>
Enterprise Risk Management (ERM) Governance

Board

Governance and Risk Committee

CEO

Corporate Audit

Risk Council

ERMC

FRMC

Centralized Risk Oversight

Executive Committee

Management

Decision Making & Risk Management

Sharon Holi, HoD Enterprise Risk, Safaricom Limited
SAFARICOM ENTERPRISE RISK MANAGEMENT POLICY

Table of contents

1. Introduction and Context ......................................................... 1
2. Management Principles ......................................................... 1
3. Risk Appetite Statement ......................................................... 2
4. Risk Tolerance ................................................................. 2
5. Responsibilities and Accountabilities (Governance Structure) .......... 3
   5.1 The Board Audit Committee .............................................. 3
   5.2 CEO ................................................................. 4
   5.3 Senior Management ....................................................... 4
   5.4 Director Risk Management and Enterprise Risk Management Team 4
   5.5 Assurance Functions - Internal Audit .................................... 4
3 Risk Appetite Statement

The risk appetite statement will act as a guide to management and staff in evaluating strategic alternatives, setting related objectives, and developing mechanisms to manage related risks. The risk appetite statement will also act as an assurance to key stakeholders of Safaricom’s commitment to managing risks. Below is the risk appetite statement for Safaricom:

“We the staff and management of Safaricom Limited are committed to growing stakeholder value by effectively and efficiently managing business risks.

We proactively manage any threats that may lead to the loss of revenue or market share by consistently delivering quality and reliable services to our customers.

As employees we are committed to conducting business with integrity while exercising zero tolerance to any losses that may occur through wastage or fraud. Our Board and management team are dedicated to the highest standards of corporate governance whilst employing world class practices that protect the reputation of our brand and company as one of Africa’s most respected organizations.”

4 Risk Tolerance
Pre-requisite of Effective ERM

Risk Management Governance
- Awareness
- Philosophy
- Tolerance/Appetite
- Organization
- Policy

Risk Management Infrastructure
- Methodology
- Tools
- Procedures

Risk Management Process
- Identification & Assessment
- Control Activities
- Risk Mitigation Action Plan
- Monitoring & Reporting
- Information & Communication

Road Map to Effective ERM Implementation

Risk Management Maturity Assessment
- ISO 31000
- ASNZS 4360
- COSO ERM
- API
- Basel II

Awareness
- Skills
- Culture
- Image
- Processes
- Confidence
- Resources
- Application
Enterprise Risk Management carries out Risk assessments twice every year in conjunction with business units and other stakeholders to determine the risk landscape of the business. The assessments identify various risks, their probability of occurrence, potential impact and the adequacy of controls put in place to manage these risks. Furthermore, planned mitigations are tracked for implementation and reported to the Board Audit Committee. The risk management process is based on International best practice standards i.e. ISO31000 and the Committee of Sponsoring Organizations (COSO) framework.

Identified risks are evaluated and rated by determining the likelihood of occurrence and impact of loss to the business in accordance to our risk tolerance levels as identified by senior management and documented in the table below. The likelihood of occurrence and impact are rated according to the rating tables below and in cognizance of the effectiveness of the existing controls. The measures of impact table is included in Appendix 1.

<table>
<thead>
<tr>
<th>Level</th>
<th>Descriptor</th>
<th>Likelihood Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Certain</td>
<td>Is expected once a week</td>
</tr>
<tr>
<td>4</td>
<td>Likely</td>
<td>Will probably occur once a month</td>
</tr>
<tr>
<td>3</td>
<td>Possible</td>
<td>Might occur once a quarter</td>
</tr>
<tr>
<td>2</td>
<td>Unlikely</td>
<td>Possibly once a year</td>
</tr>
<tr>
<td>1</td>
<td>Rare</td>
<td>Extraordinary event - might occur every 1-5 years</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Level</th>
<th>Impact Descriptor</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Extremely serious harm</td>
</tr>
<tr>
<td>4</td>
<td>Very Serious Harm</td>
</tr>
<tr>
<td>3</td>
<td>Serious Harm</td>
</tr>
<tr>
<td>2</td>
<td>Minor Harm</td>
</tr>
<tr>
<td>1</td>
<td>No significant Harm</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>RISK RATING</th>
<th>RISK ACCEPTANCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>We are not sufficiently prepared and immediate action is required</td>
</tr>
<tr>
<td>B</td>
<td>We believe Safaricom can or should do more.</td>
</tr>
<tr>
<td>A</td>
<td>We don’t believe Safaricom can or should do more</td>
</tr>
</tbody>
</table>

Sharon Holi, HoD Enterprise Risk, Safaricom Limited
Risk Universe

Possible Risks

1422. Alien Invasion
1423. City destroyed by angry Monkey God
1424. Building eaten by giant pig.

“Well he certainly does a very thorough risk analysis.”
Scope
Risk Universe

IAMGOLD Risk Universe

Organization
- Leadership
- Governance:
  - Performance
  - Oversight and authority
  - Control environment
- Human Resources:
  - Talent management (attraction and retention)
  - Succession planning
  - Compensation & benefits

Strategic
- Cost containment / reduction
- Capital allocation
- Pipeline shrinkage
- Acquisition / Dispositions
- Joint venture
- Exploration
- Capacity constraints
- Investor relations
- Erosion of relative shareholder value

Compliance
- Fraud and corruption
- Legal
- Regulatory
- Title
- Standard of business conduct

Embedded Vulnerabilities
- High All In Sustaining Costs
- Insufficient capital to develop several projects
- Limitations on debt capacity
- Declining production profile / finite resources
- Operations in higher-risk jurisdictions
- Pipeline shrinkage

Finance
- Access to & cost of capital
- Capital structure and liquidity:
  - Dividend
  - Debt level
- Taxation:
  - Strategy and planning
  - Compliance
  - Financial reporting

Operations
- Reserves and resources
  - Life of Mine (LOM)
  - Environment / sustainability
  - Mine development
  - Security
  - Health
  - Safety
  - Capital projects
  - Technical
  - Labour relations
  - IT/Network

External
- Gold price volatility
- Country / Political risk
- Energy and input volatility
- Community Engagement
- Social relations
- Competition for properties and talent
- Commodity - FX volatility
- Supply chain
- Resource nationalism
- Hostile takeover

Sharon Holi, HoD Enterprise Risk, Safaricom Limited
Pre-requisite of Effective ERM
Risk Management Process - Exercise

- Sources of information – annual report, interviews, workshops
- Gross versus net risk
- Likelihood and impact
- Adequacy of current controls
- Additional mitigations required
- Frequency of follow up
Maturity Assessment

- Continuous awareness
- Training and regular reading (CERM)
- Culture - To what extent is Risk discussed at Management decision making
- People and tools; budget to mitigate risk
- RISK ATTITUDE
Risk Management is everywhere!

Everyone is a Risk Manager
Q & A

Sharon Holi, HoD Enterprise Risk, Safaricom Limited