Capital Markets & Securities Authority

SUPERVISORY MODEL

The CMSA has adopted Risk Based Supervision to the capital market intermediaries. Traditionally, supervisors focused on rule based system that relied on review of transactions and historical performance, covering all operational areas regardless of any demonstrated or probable weakness. Subsequently it has been realized that Rule Based Supervision may not be an effective tool for preventing financial crisis. This realization has led to the emergence of the risk-based approach to supervision where emphasis is placed on the process rather than on individual transactions whereby:-

- Identifies, assesses and monitors licensed entity business conduct through off- and on-site inspections and following up on complaints and self-reported breaches.
- For high risk and high impact firms, they are generally subject to more frequent on-site inspections and closer scrutiny

Requires licensed entities to perform own risk management activities based on risks taken on by the firm and market intermediary's treatment is based on its risk profile and ability to manage the risk.

Checklist Excerpts for Risk Assessment Inspections of LDMs

The four basic elements of an effective Risk Management system include:

1. Board and senior management oversight;
2. Policies and procedures that have been developed and implemented to manage business activities effectively;
3. Risk measurement, monitoring, and management information systems that are in place to support all business activities; and
4. Establishment of internal controls and the performance of comprehensive (external and possibly internal) audits to detect any deficiencies.

i. Risk Management: Board and Management Oversight

The **Board of Directors** is responsible for setting the tone at the top, overseeing management and ensuring risk management, regulatory, compliance, and ethics obligations are met. The Board should discuss with senior management the state of the entity's risk management and provide oversight as needed. The Board should ensure it is apprised of the most significant risks, along with actions management is taking and how it is ensuring effective risk management. The Board should consider seeking input from internal auditors, external auditors, and others.

Senior Management is responsible for reinforcing the tone at the top, driving a culture of compliance and ethics and ensuring effective implementation of risk management in key business processes, including strategic planning, capital allocation, performance management, and compensation incentives. The chief executive should assess the organization's risk management capabilities. In one approach, where practical, the chief executive brings together business unit heads and key functional staff to discuss an initial assessment of risk management capabilities and effectiveness. Whatever its form, an initial assessment should determine whether there is a need for, and how to proceed with, a broader, more in-depth evaluation.

Generic questions to be answered to assess risk management control:

(NOTE: It is best practice to gain evidence to the responses of these questions. Evidence might be reports to Board; written supervisory procedures; minutes from Board meetings, etc.)

1. ***Has the organization defined and articulated a risk appetite and communicated it to employees?*** An effective risk appetite not only serves as the base for a firm's risk management framework, but also shows the CMSA that it has a clear mission statement when it comes to managing risk.

2. ***Has the firm established a strong culture of risk management?*** This means that the organization's risk appetite has been communicated to employees and daily business operations reflect it. Can it be stated that the organization's risk appetite is at the forefront of any business decision that's made?

3. ***Is risk management implemented within the organization?*** This means that risk management is part of the business workflow. Technology is a key tool because it can help shed light on risks and the firm's current risk situation. Additionally, it allows compliance, risk, IT and internal auditing departments to address risks that are important to them, while working within a common framework spanning the entire institution.

4. ***Are there experts on the Board who can effectively lead risk management efforts?*** It takes more than technology to manage risk. Firms need experts in each risk area and business unit, and must also make sure vendors and other third parties they work with know their business and the risk challenges they face.

5. How is risk management controlled and managed? Controls must be in place to help ensure the firm is complying with regulatory requirements and acting in accordance with its risk appetite. Can the firm prove to the CMSA that the firm is proactively managing and measuring risk?

Guidance Notes:

1. For a better risk management and control program, the firm should develop risk-based policies and procedures that (1) conform to the firm's actual business and activities and (2) specify who is responsible for specific tasks, who verifies or reviews that it has been done, and who approves it. In some instances, a 'completion date' should be noted as well. Risks need to be (1) identified; (2) assessed; (3) mitigated; (4) monitored; and (5) reviewed. Communications are most important within throughout the firm and between the firm and the CMSA.
2. By conducting a supervisory controls review, the firm verifies a connection between what policies and procedures are developed and what is being implemented. The Written Supervisory Procedures (WSPs) are a road map for understanding and reviewing the compliance and risk management program. Whatever is stated in the WSPs should be implemented for the oversight of the Board and Management and for the supervision of the CMSA. WSPs should be amended from time to time as necessitated.
3. Overall rating of risk management (system) would consider factors that include:
    - the extent to which the entity is able to manage all the risks and other major activities and in particular its ability to identify, measure, monitor and control these risks;
    - the soundness of the qualitative and quantitative assumptions implicit in the risk management system;
    - whether risk policies, guidelines and limits at the entity are appropriate and consistent with its trading and other activities, management personnel and experience level, and overall financial strength;
    - whether the management information system and other forms of communication are consistent with the level of business activity and complexity of products offered at the entity and provide sufficient support to monitor risk exposure and compliance with established limits accurately; and

- the ability of management to recognise and accommodate new risks that may arise from the changing environment and to identify and address risks not readily quantified in a risk management system.

4. Effective internal accounting controls and audit procedures are the underlying support for a risk management and control system. Basic internal controls such as authorization for transactions, segregation of duties, safeguards over assets and records, documentation standards, and independent verification controls should be consistent between firms. In terms of risk management and capital protection, the most consequential internal controls involve the segregation of duties between the trading function and the internal control and risk management functions and the authorization of transactions.
5. The rating for risk management, which is assigned by the on-site inspector/supervisor at the conclusion of the on-site, risk-focused inspection, is based on a scale of one to three in ascending order of supervisory concern (i.e., 3 reflects the highest perceived level of risk; 1 is the lowest level of risk). This rating is assigned to reflect findings within the four elements of sound risk management as outlined above.

Inherent Risks of Licensed Entities

The following inherent risks are associated with the licensed entities of the Tanzanian capital markets. These risks may be related to each other in some respects and may change as the capital markets develop. Each risk should be assessed and rated.

- Operational;
- Financial;
- Counterparty (or credit);
- Market and Liquidity;
- Legal/Regulatory/Compliance; and
- Systemic.

Other risks shall become more relevant with the development of the capital markets, such as Interest Rate Risk and Foreign Exchange Risk that pertain to derivatives and bonds. Although the bonds are listed for trading now on the DSE, these bonds are hardly traded.

When assessing the risks, included will be the *probability* of occurrence as well as the *impact* on the firm or on the capital markets as a whole. In addition, when rating the risk, the Risk Management system and *mitigating activities* are also considered.

As presented in the IOSCO Public Document 78:

"Market risk", inherent in any investment, is the risk that the investment will not be as profitable as the investor expected because of fluctuations in the market. Market risk involves the risk that prices or rates will adversely change due to economic forces. Such risks include adverse effects of movements in equity and interest rate markets, currency exchange rates, and commodity prices. Market risk can also include the risks associated with the cost of borrowing securities, dividend risk, and correlation risk…as well as Liquidity Risk.

"Liquidity Risk" is the risk that an owner of securities may not be able to sell or transfer that instrument quickly and at a reasonable price, and as a result, incur a loss.

"Counterparty or Credit Risk" involves the possibility that the counterparty to the transaction will not perform on its obligations. Credit risk comprises risk of loss resulting during settlement. Although not currently implemented in the Tanzanian capital markets, securities firms are faced with credit risk whenever they enter into a loan agreement, an OTC contract, or extend credit. Credit risk can be minimized by risk management and controls and procedures that require counterparties to maintain adequate collateral, make margin payments, and have contractual provisions for netting. More relevant in the current Tanzanian capital markets is that counterparty risk is mitigated if all parties in a transaction on the DSE would comply with the DSE Rules of pre-funding a purchase transaction and ensuring that the securities are on deposit prior to entering a

sales order; mitigation would also be effected through the enforcement of these rules by the DSE as well as the CMSA.

"Operational Risk" is the risk that improper operation of trade processing or management systems will result in financial loss. Operational Risk often is perceived to include "financial risk" where due to the crystallization of operational risk, the entity falls below the minimum prudential or risk based capital requirement. Operational risk encompasses the risk of loss due to the breakdown in controls within the firm including, but not limited to, unidentified limit excesses, unauthorized trading, fraud in trading or in back office functions including inadequate books and records and a lack of basic internal accounting controls, inexperienced personnel, and unstable and easily accessed computer systems. Operational risk is controlled through proper management procedures including adequate books and records and basic internal accounting controls, a strong internal audit function which is independent of the trading and revenue side of the business, clear limits on personnel, and risk management and control policies.

"Financial Risk", which can be incorporated into the more general category of Operational Risk, is the risk of losing capital, with the ultimate loss forcing the intermediary to become in capital non-compliance or go bankrupt forcing liquidation. Financial risk is related to risk based capital adequacy, which in the Tanzanian capital markets, is most effected by liquidity risk (rather than market risk), position/concentration risk, and risk of poor risk management and control activities for an intermediary. In addition, counterparty risk leads to potential financial loss due to a customer or counterparty not being able to or not fulfilling commitments. An intermediary rapidly expanding its customer base or its products for dealing and certainly for an intermediary increasing its investments in various financial products runs a financial risk where market conditions, for example, may cause financial loss. Products handled by and invested in must be understood; this may be a challenge initially when products are introduced into the Tanzanian market, e.g., commodities and derivatives. In fact, when derivatives are introduced to the Tanzanian capital markets, these can be used by intermediaries (and customers alike) to hedge...mitigate...investments in other securities. It is in the best interests of the capital market and intermediaries that the CMSA mandates early warning reports from intermediaries that, for example, are within 120% of the capital requirements. Additionally, the CMSA would mandate to all auditors who perform annual reporting for intermediaries, which they report to the CMSA directly, financial inadequacies, financial losses, and even risk management deficiencies immediately as discovered.

"Legal/Regulatory/Compliance Risk" is the risk of loss arising from unenforceable contracts and adverse judgments, negative publicity regarding an entity's business practices, or its inability or unwillingness to comply with laws, rules and regulations. It includes the propensity for an entity to be used for money laundering and terrorist financing activities. The key to the effectiveness of the compliance function is providing independent oversight of the management of the entity's compliance with all laws, regulations, codes of conduct, and standards of good practice relevant to the activities of the entity in the jurisdictions in which it operates.

"Systemic risk" refers to (1) the scenario that a disruption at a firm, in a market segment, or to a settlement system could cause a "domino effect" throughout the capital or financial markets toppling one (financial) institution after another, or (2) a "crisis of confidence" among investors, creating illiquid conditions in the marketplace. Systemic risk encompasses the risk that failure in one firm or one segment of the market would trigger failure in segments of or throughout the entire financial markets. In the Tanzanian capital markets, i.e., trading on the DSE, since this market is highly illiquid at the current time, this threat of 'systemic risk' is a constant. Systemic risk is perhaps the greatest challenge to supervisors and to the financial markets. A uniform, flexible framework of risk management and controls, coupled with adequate capital standards is essential to the continued orderly operation of the global financial markets.