Draft Risk Management Guidelines for Capital Markets in Zambia

Contents

APPROVAL OF THE RISK MANAGEMENT GUIDELINES

The Risk Management Guidelines for Capital Markets were approved by the Chief Executive Officer of the Securities and Exchange Commission on the day of 2022 in Lusaka

PHILIP K CHITALU
CHIEF EXECUTIVE OFFICER

Queries relating to this document should be referred to:

The Chief Executive Officer
Securities and Exchange Commission
Plot 3827 Parliament Road, Olympia
P. O. Box 35165
LUSAKA
☎ +260 211 227 012 or +260 211 222 368
✉ info@seczambia.org.zm

SECTION 1: INTRODUCTION

1.1 Objective of the SEC Risk Management Guidelines

1.2 In 2021, the Board of the Securities and Exchange Commission approved the Commission Risk Based Supervision Policy "RBS Policy". The RBS Policy represents the Commission's commitment to transition its supervision of Zambian Capital markets from a compliance-based regime to a risk-based supervision regime. The Commission's approach to supervision has therefore evolved to focus on the risk. Risk has been defined as the threats posed by the activities of capital market operators to the achievement of the Commission's core supervisory objectives. Under Sub-section 9(1) of the Act, the Commission's mandate is to create and promote conditions in the capital markets aimed at ensuring an orderly growth, integrity, and development of the capital markets. Sub section 9(2) spells out further functions of the Commission which include matters specific to the conduct of CMOs such as to:

- promote and encourage high standards of investor protection and integrity among
- participants in the capital markets;
- support the operation of free, orderly, fair, secure, and properly informed capital
- markets;
- take all reasonable steps to safeguard the interest of persons who invest in securities
- and guard against illegal and improper practices as provided in this Act;
- provide, promote, or otherwise support financial education, awareness and
- confidence regarding financial products, institutions, and services.

1.3 The Commission approach to supervision under the RBS Policy also places emphasis on holding the Board and Senior Management accountable for the results of the CMO's activities. The CMO's Board of Directors and Senior Management are responsible for the strategic management and direction of the CMO and are responsible for ensuring that the conduct of the CMO and that of its employees meet the standards required for investor protection.

1.4 These guidelines are intended to provide the minimum standards for risk management for capital markets operators. They are not an exhaustive guide to risk management and therefore, the Board and Senior Management are expected to put in place policies and procedures aimed at ensuring that the CMO develops and implements a risk management framework that is in the best interests of the CMO and all relevant stakeholders taking into account the CMO's business model, its operating and legal environment, and any other factors as the Board deems fit.

1.5 Definitions

In these Guidelines, unless the context otherwise requires-

'CMO' shall have the same meaning as contained in the Securities Act.

'board' means the board of directors of a CMO, or an equivalent body charged with the governance of the CMO.

'Chief executive officer' or 'CEO' means a person responsible, under the immediate authority of the board of directors for the conduct of the business of a CMO.

'Chief financial officer' or "CFO" means the individual charged with the primary responsibility for managing the company's finances, which may include including financial planning, management of financial risks, record-keeping, and financial reporting.

'Chief risk officer' "CRO" means an independent officer with the responsibility for a CMO's risk management function and its enterprise-wide risk management framework.

'Compliance officer' or **'Chief Compliance Officer"** means a senior staff member with overall responsibility for coordinating the identification and management of the CMOs compliance risk and for supervising the activities of staff discharging the compliance function.

'CMO' or 'Capital Market Operator' shall have the same meaning as contained in the Securities Act

'Insider' shall have the same meaning as contained in the Securities Act.

'Internal control' means a process effected by the institution's board of directors, management and other personnel designated to provide reasonable assurance regarding the achievement of the CMO's objectives such as effectiveness of the risk management process, reliability of financial reporting and compliance with applicable laws and regulations.

'Internal audit' means an independent, objective assurance and consulting activity designed to add value and improve an organization's operations and which helps an organization accomplish its strategic objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

'non-executive director' means a member of the board who is not involved in the day-to-day management of the CMO and is not a full-time salaried employee of the institution.

'Risk appetite' means the aggregate level and types of risk a CMO is willing to assume, decided in advance and within its risk capacity, to achieve its strategic objectives and business plan.

'Risk profile' means a point in time assessment of the CMO's risk exposures based on current or forward-looking assumptions.

'Senior management' or **'management'** means- the executive committee or management team comprising a core group of individuals who are responsible and accountable to the board for effectively overseeing the day-to-day management of the CMO.

'Significant activities' refers to a line of business, business unit or process that is fundamental to the CMO's business model and its ability to meet its strategic objectives such that if that activity is not well managed, the CMO risks not being able to meet its corporate goals.

'Stakeholder' means an individual or group, in addition to shareholders, who have an interest in, and/or influence over, the CMO's operations and the achievement of the institution's goals, such as creditors, employees, suppliers, customers, the Regulators, Government and Quasi-Government Bodies, the Community etc.

1.6 Application of these guidelines

1.6.1 These Directives shall apply to all Capital Markets Operators taking into their size and nature of business operations. The code shall be compulsory for the following types of capital markets operators:

- Dealers
- Investment Advisers
- Securities Exchanges
- Clearing and Settlement Agencies

- Share transfer agents
- Credit Rating Agencies
- Other CMOs as determined by the Commission

1.6.2 Issuers of registered Securities who are not licensees will need to make a determination to what extent these guidelines are relevant in the context of ensuring they comply with the continuing obligations imposed by the Securities Act and the rules of the exchange they belong to.

1.7 Principles-Based vs Rules-Based Approach

1.7.1 In these guidelines the Commission has adopted a principles-based rather than a rules-based approach. A principles-based approach provides CMOs with the flexibility to adopt systems and procedures that suit their individual circumstances. However, when completing the Self-Assessment Questionnaires each CMO must provide factual explanations which must be backed by documentary evidence. The Commission will place limited reliance on representations from the Board or Senior Management as to the existence or effective operation of the CMO's Quality of Risk Management Framework.

1.7.2 Further, whilst CMOs may wish to ascertain the level of risk, the Commission's emphasis is not on the Risk Rating from the CMO's point of view, but on the existence and effective operation of identified inherent risks.

SECTION 2: RISK MANAGEMENT FRAMEWORK

2.1 Inherent risk

2.1.1 Inherent risk is the probability of material loss to investors due to exposure to, and uncertainty arising from, current and potential future events arising from the undesirable market conduct practices of a CMO or its representatives/agents. Inherent risk is driven by the nature and extent of the business activities of the CMO. Therefore, the Board and Senior Management must have a thorough understanding of both the nature of the CMO's activities and the environment in which these activities are undertaken is essential to identify and assess inherent risk.

2.2 Risk Categories

2.2.1 The Commission uses the following categories to assess inherent risk:

(1) Conduct risk
(2) Credit risk;
(3) Market risk;
(4) Operational risk;
(5) Legal and Regulatory risk;
(6) Strategic risk; and
(7) Money Laundering/ Terrorist Funding Risk (ML/TF Risk);

2.3 Risk Management Function

2.3.1 In accordance with the SEC Code of Corporate Governance and as part of the implementation of RBS in the Zambia Capital Markets, each CMO is required to establish an independent Risk Market Function ("RMF") and appoint a Chief Risk Officer. The RMF and the CRO will supervise the CMO's risk management processes as outlined below. The function should be independent from those who take or accept risks on behalf of the institution and should report directly to the board or a committee of the board.

2.3.2 The risk management function should be responsible for ensuring that effective processes are in place for:

(i) Identifying current and emerging risks;
(ii) Developing risk assessment and measurement systems;
(iii) Establishing policies, practices, and other control mechanisms to manage risks;
(iv) Developing risk tolerance limits for Senior Management and board approval;
(v) Monitoring positions against approved risk tolerance limits; and
(vi) Reporting results of risk monitoring to Senior Management and the board.

2.4 Risk Management Process

2.4.1 Regardless of the Risk Management Programme design, each programme should include:

(1) **Risk Identification:** Risk identification should be a continuous process and risk CMOs are encouraged to identify and have a thorough understanding of their key business activities and processes and assess how these give rise to inherent risks. Risk identification should also consider the characteristics of the CMOs product and services, delivery channels, customers, etc. CMOs are expected to focus on significant activities when undertaking risk identification exercises.

(2) **Risk Measurement:** Once the risks associated with a particular activity have been identified, the next step is to measure the significance of each risk. Each risk should be viewed in terms of its three dimensions: size, duration, and probability of adverse occurrences. Accurate and timely measurement of risk is essential to effective risk management systems. CMOs are expected to focus on key risks within the significant activities of the CMO. The CMO is also expected to monitor other risks.

(3) **Risk Control:** the CMO should put in place controls to manage/ mitigate key inherent risks to prevent or minimize the adverse consequences. This can be achieved by:

- avoiding or placing limits on certain activities/risks,
- mitigating risks and/or
- offsetting risks.

This should be done by establishing and implementing controls at the first line of defense which is Operational Management. This is done by implementing policies and procedures for undertaking key significant activities. Further, CMO's are expected to enhance controls established by operational management by establishing oversight sight functions namely Risk Management Function, Compliance Function, and Internal Audit Function. Board and Senior Management also form part of the controls structures by providing oversight over the CMOs risk management process.

(4) **Risk Monitoring:** CMOs should establish Management Information Systems (MIS) that accurately identify and measure risks at the inception of transactions and activities. Information and communication are vital for monitoring significant changes in risk profiles. Monitoring risks means developing reporting systems that identify adverse changes in the risk profiles of significant products, services and activities and monitoring changes in controls that have been put in place to minimize adverse consequences. Information and communication controls should be designed to cut across the organization from operational management to the Board.

2.5 Basic elements of a sound risk management system

2.5.1 The risk management program of each institution at minimum contains the following elements of a sound risk management system:

(i) Active Board and Senior Management Oversight
(ii) Organizational structure
(iii) Adequate Policies and Procedures

(iv) Adequate Risk Monitoring and Management Information Systems (MIS)
(v) Adequate Internal Controls

2.5.2 Active Board and Senior Management Oversight

The SEC RBS Policy emphasizes Board and Senior Management accountability for the level of risk assumed by the CMO in conducting its business operations. The Board is responsible for approving the overall business strategies and significant policies of their organizations, including those related to managing and taking risks. The Board should ensure that senior management is fully capable of managing the activities that their institutions conduct. To achieve this, the directors are responsible for understanding the nature of the risks significant to their organizations and for ensuring that the management is taking the steps necessary to identify measure, monitor and control these risks.

2.5.3 Senior management is expected to provide regular reports that identify the size and significance of the risks in terms that are meaningful to the directors. Directors should also be proactive by developing an appropriate understanding of the risks their institution face including consulting with technical experts and other professionals e.g., auditors, financial experts, valuers etc. Based on this understanding, the directors should provide clear guidance regarding the level of exposures acceptable to their institutions and have the responsibility to ensure that senior management implements the procedures and controls necessary to comply with adopted policies.

2.5.4 Senior management is responsible for implementing strategies in a manner that limits risks associated with each strategy. Management should therefore be fully involved in the activities of their institutions and possess sufficient knowledge of all major business lines to ensure that appropriate policies, controls, and risk monitoring systems are in place and that accountability and lines of authority are clearly delineated. Senior management is also responsible for establishing and communicating a strong awareness of and need for effective internal controls and high ethical standards. Meeting these responsibilities requires senior managers of institutions to demonstrate a thorough understanding of developments in the capital markets and a knowledge of the activities their institution conducts, including the nature of the internal controls necessary to limit the related risks.

2.5.5 Adequate Policies and procedures

The board of directors and senior management should tailor their risk management policies and procedures to the types of risks that arise from the activities the institution conducts. Once the risks are properly identified, the institution's policies and procedures should provide detailed guidance for the day-to-day implementation of broad business strategies and should include limits designed to shield the organization from excessive and imprudent risks.

2.5.6 Policies and procedures should:

- Provide for adequate and timely identification, measurement, monitoring, control, and mitigation of the risks posed by the CMO's significant activities.
- Ensure that the economic substance of a CMO's risk exposures is fully recognized and incorporated into the CMO's risk management systems.
- Be consistent with the CMO's stated goals and objectives, as well as its overall financial strength.
- Clearly delineate accountability and lines of authority across the CMO's various business activities and ensure there is a clear separation between business lines and the oversight functions (Risk, compliance, and audit functions).
- Include escalation procedures to address breaches of prescribed controls/ limits.
- Provide for the review of new businesses and products by bringing together all relevant risk management, control, and business lines to ensure that the CMO is able to manage and control the activity prior to it being initiated. and
- Include a schedule and process for reviewing the policies, procedures, and limits and for updating them as appropriate. CMOs are encouraged to develop a system of mapping policies and procedure documents to its significant activities to ensure all key aspects of the business are covered.

2.5.7 Adequate Risk Monitoring and Management Information Systems (MIS)

Effective risk monitoring requires CMOs to identify and measure all material risk exposures. Consequently, risk-monitoring activities must be supported by information systems that provide senior management and the board with accurate and timely reports on the financial condition, operating performance, and risk exposure of the institution.

2.5.8 The sophistication of risk monitoring and MIS should be consistent with the complexity and diversity of the institution's operations. Every CMO should develop a set of management and board reports to support risk-monitoring activities. The complexity and detail of these reports should be tailored to the needs of senior management and the Board. Typically, these reports will include:

- Periodic Statements of financial position, balance sheets and income statements;
- Statement on investment limits and prohibitions
- Operational reports on market activity (e.g., trading reports)
- Compliance reports
- Other relevant reports.

2.5.9 To ensure effective measurement and monitoring of risk and management information systems, Senior Management must ensure that the following standards are observed:

(i) the CMO's risk monitoring practices and reports must address all its material risks;

(ii) key assumptions, data sources, and procedures used in measuring and monitoring risk should be appropriate and adequately documented and tested for reliability on an ongoing basis;

(iii) appropriate periodic stress testing should be conducted and management action plans to mitigate the risks identified in the Stress Tests are put in place.

(iv) The CMO's information and communication processes (including reports and communication channels) should be consistent with its activities, structured to monitor exposures and compliance with established limits, goals, or objectives and, as appropriate, compare actual versus expected performance and;

(v) The Board and Senior Management should have access to accurate and timely information to enable them to undertake their roles and responsibilities. Information at a minimum should contain sufficient information for decision-makers to identify any adverse trends and to evaluate the level of risk faced by the institution. Information to the Board should also include updates to the extent necessary on key decisions/ directives made by the Board and/ or Senior Management. Unclosed/ Outstanding actions from Board/ Senior Management meetings should be clearly documented to evidence the Board/ senior management's role in addressing the specific risk events identified.

2.5.10 Adequate Internal Controls

A CMO's internal control structure is critical to the safe and sound functioning of the organization, in general and to its risk management, in particular. Establishing and maintaining an effective system of controls, including the enforcement of official lines of authority and the appropriate separation of duties is one of management's important responsibilities.

2.5.11 The system of internal controls should promote effective operations and reliable financial and regulatory reporting, safeguard assets and ensures compliance with relevant laws, regulations, and institutional policies. Internal controls should be tested by an independent and suitably qualified internal auditor who reports directly to the Board. The results of audits or reviews, conducted by an internal auditor or other person and management's responses should be documented. In addition, communication channels should exist that allow the Internal audit to report negative or sensitive findings directly to the Board.

2.5.12 To ensure the adequacy of the CMO's internal controls, the following standards should be observed: -

(i) The system of internal controls should be appropriate to the type and level of risks posed by the nature and scope of the institution's activities.

(ii) The institution's organizational structure should establish clear lines of authority and responsibility for monitoring adherence to policies, procedures, and limits.

(iii) Reporting lines should provide sufficient independence of the control areas from the business lines and appropriate segregation of duties throughout the institution such as those relating to trading, custodial, and back-office activities.

(iv) Official institutional structures should reflect actual operating practices.

(v) Financial, operational, and regulatory reports should be reliable, accurate and timely; wherever applicable, exceptions are noted and promptly investigated.

(vi) Adequate procedures for ensuring compliance with applicable laws and regulations should be in place.

(vii) The Risk Management, Compliance and Internal audit Functions should provide for independence and objectivity of the oversight function.

(viii) Internal controls and information systems should be reviewed and tested regularly. The coverage, procedures, findings, and responses to audits and reviews should be documented. Senior Management should ensure material weaknesses are addressed by ensuring actions to address weaknesses are objectively verified and reviewed.

(ix) The institution's audit committee or board of directors should review the effectiveness of internal audits and other oversight functions on a regular basis.

SECTION 3: CONDUCT RISK

3.1 Definition of Conduct Risk

3.1.1 Conduct risk is the risk that the conduct of the CMO and/ or its employees will result in poor outcomes for investors and/or other stakeholders. Conduct risk may also arise from market abuses/malpractices in Financial Market Infrastructures (Exchanges, CSDs etc.). Market abuses include insider dealing, stock price manipulation (e.g., pump and dump schemes). In market abuse, information asymmetry allows one party to take advantage of another person's lack of knowledge about the transaction they are being asked to participate in. Good outcomes can be defined as customers getting financial services and products that meet their needs.

3.1.2 Under the Securities Act "market misconduct" includes the following:

- the use or disclosure of price-sensitive information contrary to this Act;
- engaging in improper trading practices as provided in Part XVIII;
- failure to comply with any provision of this Act; and
- a conviction of an offence under this Act;

3.1.3 Treating Customers Fairly (TCF) is an approach designed to ensure that CMOs have policies and procedures designed to produce fair outcomes for its customers. CMOs should deliver the fair outcomes to their customers throughout the product life cycle, from product design and promotion, through advice and servicing, to complaints and claims handling. Some of these outcomes can be summarized as follows:

(i) Sufficient disclosures: provide sufficient and non-misleading disclosure to investors entering financial contracts and making investment decisions. This includes clear disclosure of the terms and conditions, and/or applicable rules, relating to contracts and trading relationships including fees, treatment of complaints and venues for redress;

(ii) Suitability of financial products: products supplied to investors are the best considering their risk profile and financial objectives;

(iii) Services provided by Fit and Proper persons – investors are not exposed/ attended to by unlicensed and incompetent persons when obtaining financial services;

(iv) Safety of customer assets: prevent mishandling or expropriation of customer funds and assets;

(v) Avoidance of conflicts of interest: Avoid, prevent, or manage conflicts of interest; ensure the provision of un-conflicted advice suitable and appropriate to customers' credit circumstances and financial objectives

(vi) Avoidance of improper market practices/ market abuse: such as discourage improper inducements or incentives;

(vii) Protect confidentiality and data: The data protection Act makes provision for the protection of customers referred to as "data subjects" and are defined as individuals from, or in respect of whom, personal information is processed.

(viii) Operate with appropriate resources; and in general

(ix) **Treating customers, counterparties, and the markets fairly:** The CMO must not engage in market misconduct and market manipulation schemes which harm investors and others.

(x) **Best execution:** CMOs should seek the best outcome for their clients by choosing and executing the best available option in a timely and fair fashion.

3.1.4 The above outcomes are reiterated in the Statement of Principles in Rule 4 of the Securities (Conduct of Business) Rules, Statutory Instrument 168 of 1993.

Rule 4: Principles of best practice

In his conduct of securities business, a licensee shall at all times act according to the principles of best practice and, in particular, shall-

(a) observe high standard of integrity and fair dealing;
(b) act with due skill, care, and diligence;
(c) observe high standards of market conduct;
(d) seek from customers information about their circumstances and investment objectives which might reasonably be expected to be relevant in enabling him to fulfil a licensee's responsibilities to his customer;
(e) take reasonable steps to give every customer he advises, in a comprehensible and timely way, any information needed to enable the customer to make a balanced and informed investment decision;
(f) avoid any conflict of interest with his customers and, where such a conflict unavoidably arises, to ensure fair treatment to his customer by complete disclosure or by declining to act; furthermore, he should never unfairly place his interests above those of his customers;
(g) protect properly, by way of segregation and identification, those customer assets for which a licensee is properly responsible;
(h) maintain adequate financial resources to meet his securities business commitments and withstand the risk to which his business is subject;
(i) organize and control his internal affairs in a responsible manner;
(j) keep proper records;
(k) have adequate arrangements to ensure that all staff employed are suitable, adequately trained and properly supervised, together with well-defined compliance procedures; and
(l) deal with the Commission in an open and co-operative manner and keep the Commission informed of anything concerning the licensee that might reasonably be expected to be disclosed to it.

3.1.5 The table below provides examples of misconduct and offences that arise if the CMO does not manage its conduct risk well:

Type of Conduct Abuse	Examples of market conduct offences (Source: Conduct: Prevention, Detection and Deterrence of Abuses by Financial Institutions)
Selling	• Cold Calling and aggressive practices; • Failure to provide disclosure • Misrepresentations; misleading, incomplete information • Discounting disclosure (verbal lulling or over-riding of written or require ed verbal disclosure) • Sale of products unsuitable for a client's credit or risk profile • Improper account documentation

	• Failure to provide, or to timely provide, post-sale/post trade disclosure of prices or trade confirmations • Toxic, flawed or unduly complex products • Failure to provide "best execution"
Trading	• Market manipulation; • Trading ahead; front-running a customer with a proprietary trade • Misallocation • Manipulation of prices (pump and dump schemes, spoofing and layering • Insider trading • Unauthorized trading; disregard of investment policies • Disruptive, non-conventional practices as defined by exchange rule or otherwise • Unconscionable fees or mark-ups • Untimely execution • Untimely confirmation
Advising	• Conflict of interest • Mis-valuation, or different valuations for the customer and the seller • Unsuitable recommendation for financial/credit circumstances and/or financial objectives of customer • Churning (excessive trading to generate fees) • Unconscionable fees • Inappropriate compensation
Treatment of customer assets	Mishandling (e.g., failure to segregate customer and proprietary assets) Theft

3.2 Conduct Risk Drivers

3.2.1 In assessing its Conduct Risk exposures, the CMO should consider the following key drivers

(1) **CMO's Target market:** e.g., customer mix, degree of customization of product e.g., mass market vs High Net Worth;

(2) **Product design:** complex products give risk to higher conduct risk as customers are less likely to appreciate the complexity of the product being offered;

(3) **Delivery channel:** where sales are outsourced to third parties such as agents/ distributors/ aggregators, the CMO has less supervisory control over the conduct of third parties; Direct access driven by technology also affects Conduct risk depending on the circumstances;

(4) **Economic and Market trends:** This is a driver for all inherent risks as a downside in the economy emphasizes the risks faced by the CMO.

3.3 Focus areas for management of conduct risk

3.3.1 Each CMO is expected to establish policies and procedures that enable it to manage conduct risk. The conduct of business rules highlights the following areas in which the CMO should implement policies and procedures for ensuring:

(1) Management of conflicts of interest
(2) Free and fair communications to existing and potential clients.
(3) Disclosure of fees and charges
(4) Client agreements
(5) Ensuring confidentiality of customer information
(6) Suitability of financial products
(7) Customer statements and other periodic information
(8) Supervision of employees
(9) Treating customers fairly
(10) Avoiding market misconduct practices

3.3.2 Guidelines for each of these aspects are detailed from section 3.4 below.

3.4 Conflict of Interest

3.4.1 Managing conflicts of interest requires a CMO to identify and document the conflicts of interest that are likely to occur during its business. Conflicts of interest may arise from the following:

(1) Lack of independence by the CMO

Rule 5 - Independence

Where a licensee is advising or acting for a customer-
he shall not claim he is independent or impartial if he is not; and
he shall ensure that any claim he makes as to his independence or impartiality adequately includes any limitation that there may be on either.

(2) The CMO having Material Interest in the transaction directly or indirectly

Rule 6 - Material Interest

Where a licensee has a material interest in a transaction to be entered into with or for a customer, or a relationship which gives rise to a conflict of interest in relation to such a transaction, the licensee shall not knowingly either advise, or deal in the exercise of discretion, in relation to that transaction unless he has-

(a) fairly disclosed that material interest or relationship, as the case may be, to the customer; or
(b) taken reasonable steps to ensure that neither the material interest nor relationship adversely affects the interests of the customer.

(3) The CMO and its employees offering or receiving inducements in relation to their work.

Rule 7 - Inducements

A licensee must take reasonable steps to ensure that neither he nor any of his employees or agents either offers or gives, or solicits or accepts, any inducement that is likely to conflict with any duties owed to customers.

3.4.2 This means that they must consider the issue of conflict of interests so that any potential effect on decision-making is eliminated; how they do this will depend on the circumstances.

- In cases of serious conflicts of interest, it may mean the firm deciding to remove the conflict by declining to act.
- Where firms have decided against removal of the conflict of interest, they must prevent it from affecting their decision in a different way. They should disclose the conflict to the client if it can be managed and follow the policies developed to minimize damage to the client and to put the client's interests ahead of their own.

3.4.3 A firm should adopt and document appropriate policies to minimize any conflicts by identifying the instances where it would refuse to act and, where this is not necessary, making arrangements to minimize the risk of any loss to the client. The CMO should:

- Establish a conflict-of-interest policy, and adopt and document procedures, including the erection of information barriers, barriers between information technology systems, physical barriers, or even separate office locations, to minimize the possibility of information from one client being used for the benefit of another client, its employees, or the market intermediary;
- obtain undertakings from employees that they will not use information gained from the clients for their personal benefit. CMOs should institute procedures for obtaining acknowledgement from its employees and contractors that they have complied with its conflict-of-interest policy e.g.: Annual Independence declarations by the firm and its staff, Declarations in relation to the client being attended, Declarations of interest in particular market transaction;
- train employees in matters relating to the conflict of interest and the procedures developed to avoid them.
- not take advantage of information it obtained from providing services to a client for its own benefit or the benefit of its employees or for the benefit of another client
- take reasonable steps to ensure that neither it nor any of its employees or agents offers or gives, or solicits or accepts, any inducement that is likely to conflict with any of the duties owed to clients.
- Put in place procedures to disclose conflicts of interest including measures taken to manage them.
- The CMO should establish procedures for documenting and evidencing their application of the above procedures e.g.:
  (1) Having specific questionnaires where employees can document how they have handled potential and actual conflicts of interest when on-boarding new clients
  (2) When reviewing whether to continue a relationship with a client
  (3) When undertaking transactions for or on behalf of a client or others where there might be a conflict of interest

(4) The documentation must make provision to document the CMO's escalation procedures with limits defined for areas requiring Board, senior and middle management sign offs for management of conflicts of interest.

3.5 Free and fair communications

3.5.1 The CMO must ensure that there are sufficient disclosures when communicating with existing or potential clients including face-to-face meetings, calls, electronic media, new issues and marketing material.

Rule 8 - Issue of advertisements

Where a licensee issues an advertisement concerning his securities business, he shall take all reasonable steps to ensure that-

(a) the contents and presentation of the advertisement are demonstrably fair and not misleading;
(b) the advertisement discloses fairly the risks concerned.

Rule 9 - Identification of issuer

Where a licensee issues an advertisement concerning securities business, he shall ensure that the advertisement identifies him as the advertiser.

Rule 10 - Fair and clear communications

(1) A licensee may make a communication with another person which is designed to promote the provision of securities services only if he can show that he believes on reasonable grounds that the communication is fair, comprehensive, and not misleading.
(2) A licensee shall take reasonable steps to ensure that any agreement, written communication, notification, or information that he gives or sends to customers to whom he provides securities services is presented fairly and clearly.

Rule 12 - Information about the licensee

A licensee shall take reasonable steps to ensure that a customer to whom he provides securities services is given adequate information about his identity and business address and the identity and status within the licensee's firm of employees and other relevant representatives with whom the customer has contact.

Rule 13 - Information about collective investment schemes

Before or when making a personal recommendation to a customer to invest in a collective investment scheme, a licensee shall give him-

(a) information about the scheme which is adequate to enable him to make an informed investment decision;
(b) appropriate written particulars.

3.5.2 Before buying or investing in a product or instrument, clients should have key information regarding the investment that is provided at a time when they have the opportunity to consider the information and make an informed decision about whether to buy or invest. Information should be presented in a manner that investors can easily understand the features, benefits, and risks of an investment and that enables them to make better-informed decisions about their investments. The Rules also require the clients to be provided with information about the service provider

3.5.3 Some key practical considerations when communicating with clients include ensuring:

- The style of presentation enables the intended clients to understand the material by using plain language.
- The features of the investment and any associated guarantees and rights of cancellation or withdrawal should be clearly explained.
- The charges associated with the product and any costs of investment or commissions payable should be clearly disclosed.
- Communications should not emphasize the potential benefits of an investment without also giving a fair and prominent indication of any risks.
- Communications should not disguise, obscure, or hide important items, statements, or warnings.
- Information on potential future performance should be based on robust and justifiable performance data and should reflect the nature and risks of the specific type of investment.
- Distinguish between fact and opinion in the presentation of investment analysis and recommendations.

3.5.4 CMOs are referred to the Securities (Advertisements) Rules, Statutory Instrument 166 of 1993 which provide additional guidance on advertising. Appendix I is a template CMOs can use to ensure advertising materials meet the standards. Documents such as a Key Facts Statements can also be used for products such as Collective Investment Schemes.

3.6 Disclosures of fees and charges

3.6.1 Fees and charges should be disclosed to investors at all stages of engagement including:

- In marketing and promotional materials
- In client agreements, deal notes, contract notes and statements of account
- No hidden charges so that "what you see is what you will get"
- Avoid complex basis for computation of fees
- Exit and punitive charges should be discouraged, and where inevitable, they should be prominently disclosed to clients

Rule 19 – Charges

(1) A licensee's charges shall not be unfair in their incidence or unreasonable in their amount having regard to all relevant circumstances

(2) Before a licensee provides securities services to a customer it shall disclose to him the basis or amount of the licensee's charges for the provisions of those services and the nature of and amount of any other remuneration receivable by him and attributable to them.

3.7 Client Agreements

3.7.1 CMOs should formalize their relationship with clients by entering a written contract when providing services to clients. The contract will define the Terms and Conditions under which the CMO will offer its services including a description of the services to be provided and the rights and obligations of the firm to the client.

Rule 15 - Where written customer agreement required

(1) A licensee shall not provide to a customer any securities services relating to-
  (a) the discretionary management of a portfolio; or
  (b) any other type of business that is prescribed by the Commission, except under a written agreement signed by the customer and returned to licensee.

(2) The Commission and a licensed securities exchange may from time to time prescribe special procedures relating to the operation of discretionary accounts and every licensee must follow such special procedures or shall secure that such special procedures are followed.

Rule 16 - Customer agreements

(1) Where a licensee provides securities services to a customer on written contractual terms (whether pursuant to rule 15 or otherwise), the agreement shall set out in adequate detail the basis on which those services are provided.
(2) The High Court may, if it considers it just and equitable to do so, by order set aside or vary an agreement entered into in contravention of this rule, but no such order affects any dealing or transaction entered into or carried out by the licensee on behalf of the customer.

3.7.2 The contents of these Agreement can contain some of the following details:

AREA	SUGGESTED ELEMENTS
General Information	• Essential information about the market intermediary, including its name, address, and contact information.
Services	• The services to be provided. • The obligations of the market intermediary. • The obligations of the client, including how instructions are to be given.
Charges	• The fees to be charged or the way the fees will be calculated. • Any commissions to be received from third parties in relation to the services provided to the client.
Rights of the Client	The right to: • Receive title for any securities purchased. • Receive payment for securities sold within a specified period. • Receive a statement of all fees and charges. • Information on the remuneration received by the market intermediary from third parties. • Ask for information on the experience, qualifications, and disciplinary history of the market intermediary. • Receive interest on funds held by the market intermediary on the client's behalf. • See the market intermediary's conflict of interest policy. • Complain and to have that complaint dealt with fairly and promptly.

Client Assets	• The arrangements made for securing the title to, and for the custody of securities including the use of nominee accounts and a custodian, where appropriate.
Conflicts of Interest	• Any conflicts of interest relating to the market intermediary and its dealings with the client. • Any connections with third parties that could affect the services being provided, including a requirement that the market intermediary deals through certain third parties or recommends certain investment products.
Other Items	• Any other terms and conditions of the agreement, including the notice to be given in respect of any changes to it or its termination. • The fact that the SEC regulates the market intermediary.

3.7.3 CMOs should not seek to limit their liability to the detriment of their clients. This is prohibited under Rule 17 of the conduct of Business Rules.

Rule 17 - Customers' rights

(1) licensee shall not, in any written communication or agreement, seek to exclude or restrict-
- (a) any duty or liability to a customer which he has under the Act, or any subsidiary legislation made thereunder;
- (b) any other duty to act with skill, care and diligence that is owed to a customer in connection with the provision to him of securities services;
- (c) any liability owed to a customer for failure to exercise the degree of skill, care and diligence that may reasonably be expected of him in the provision of securities services.

(2) A purported exclusion or restriction prohibited by this rule shall be void and of no effect.

3.8 Client Confidentiality

3.8.1 CMOs should adopt and document policies and procedures to preserve the integrity clients and third parties confidential and secure.

Rule 33 - Customer confidentiality

(1) Subject to subrule (2), all information in the possession of a licensee relating to a customer shall be kept confidential by the licensee.

(2) A licensee may disclose information relating to a customer when properly required to do so by the Commission, a clearing house, or the market supervision department of a licensed securities exchange of which he is a member, or if he is ordered to do so by a court of competent jurisdiction or other due process of law.

3.8.2 The policies and procedures adopted could include:

- a requirement that employees undertake to maintain confidentiality, in their contract of employment or in periodic declarations;

- how to determine the employees who may have access to confidential information – logical and physical access controls to systems and premises, access levels should be established;
- procedures that effectively restrict access to confidential information by employees through the use of secure document management;
- storage systems and encryption protected information, within the market intermediary's information technology system;
- systems designed to safeguard the integrity of any electronic record or transaction recording system.
- Independent legal review of standard contracts, with detailed reviews reserved for non-standard contracts/ agreements

3.9 Suitability of financial products

3.9.1 The CMO should develop a structured methodology for providing its services including how investment decisions are made and communicated to clients.

3.9.2 At the core of the suitability of financial products are the following principles:

- principles of prioritizing the client's best interest
- Managing conflicts of interest
- Maintaining independence
- Ensuring Clients understand the product being offered

Rule 11 - Customer's understanding of risk

A licensee shall not-

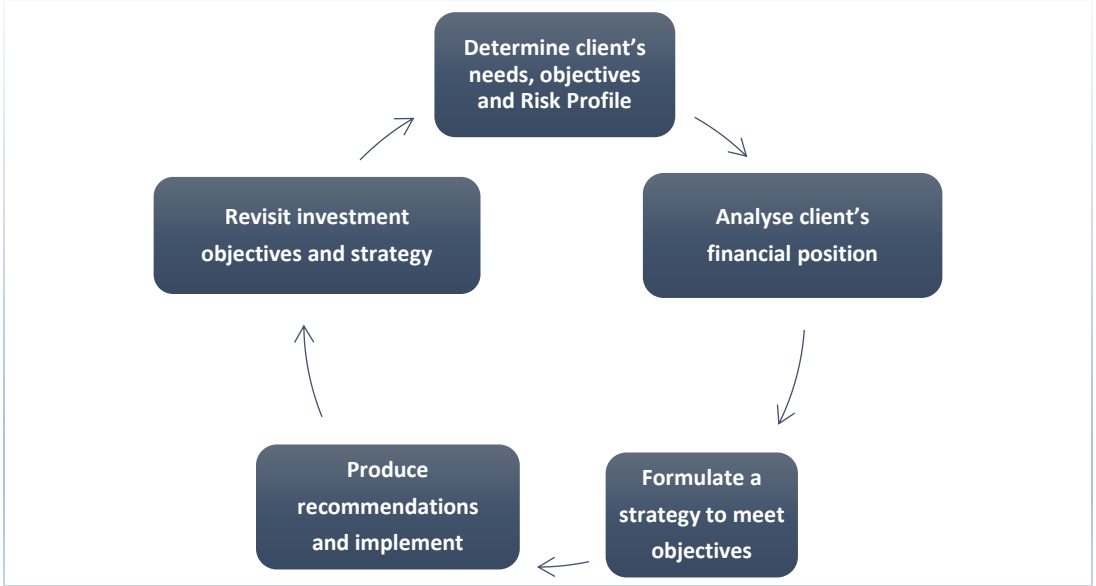
(a) recommend a transaction to a customer, or effect a discretionary transaction with or for him, unless he has taken all reasonable steps to enable the customer to understand the risks involved;
(b) mislead a customer as to any advantages or disadvantages of a contemplated transaction; or
(c) promise a return unless such return is contractually guaranteed.

Rule 18 - Suitability

A licensee shall take all reasonable steps to ensure that he does not give securities advice to, nor effect a discretionary transaction with or for, a customer unless that advice or transaction is suitable for him having regard to the facts disclosed by that customer and other relevant facts about the customer of which the licensee is or ought reasonably to be aware.

3.9.3 A typical investment advisory process is as follows:

(1) Determine client's needs, objectives, and Risk Profile
(2) Analyze client's financial position
(3) Formulate a strategy to meet client objectives
(4) Produce recommendations and implement
(5) Revisit investment objectives and strategy



3.9.4 Know Your Customer ("KYC")

3.9.5 CMOs should obtain sufficient information about its customers to enable it give suitable advice. If a CMO is acting as a discretionary investment manager for a customer should ensure that it has sufficient information to enable it to select suitable investments for the customer's portfolio.

3.9.6 To do this, CMOs must avoid one size fits all approach as investors have varying objectives and expectations. The purpose of gathering information about the client is so that financial plans can be devised, and appropriate recommendations made. The types of information that should be gathered include:

Information to be collected from/ about the client	Why Needed
Personal Details: Name; Address; age; health; family and dependents	• Details of the client's name and address will need to be verified to comply with anti-money laundering requirements. • The client's stage of life they have reached may have implications for any asset allocation strategy. It will also give an indication of their potential viewpoint on long- term investments.
Health Status	• The client's health may influence the investment strategy and allocations to cash, bonds, and equities. • If they are in good health, it may indicate a need to generate a growing level of income for many years. If they are in poor health, it may drive an investment strategy to produce a more immediate income. • A client's health may also influence their attitude to risk.

Details of Family and Dependents	• This may equally impact the client's investment objectives and attitude to risk. • It may also indicate a need to fund immediate or future spending on areas such as schooling or weddings.
Details of Occupation, Earnings, and other Sources of Income	• Existing income will impact the level of income that needs to be generated from a portfolio and the level of risk that the client is able to tolerate. • The client's occupation or business will give a good indication of their experience in business matters which may be relevant when judging the suitability of a particular type of investment that carries greater risk and where the firm is required to assess the client's experience before recommending it.
Present and Anticipated Outgoings	• This will be needed in conjunction with their income, where it is necessary to look at budgeting, planning to meet certain liabilities or generating a specific income return. • liquidity and time horizons - immediate needs; known future liabilities; need for an emergency reserve
Assets and Liabilities	• Full details of the client's assets and liabilities are clearly needed. • In addition, details will be needed of where assets are held, their tax treatment, acquisition costs and details of any early encashment penalties.
Any Pension/ Insurance arrangements	• The pension arrangements the client has made will need to be closely linked to the investment strategy that is adopted both for retirement and other financial objectives.
Potential Inheritances and any Estate Planning Arrangements, such as a Will	• This will be relevant if the amounts due to be inherited might influence the investment strategy adopted. • The adviser should also check whether the client has left any specific gifts of shares in their will and, if so, whether this would prevent any sale of such a holding.
Investment objectives	• growth; protecting real value of capital; generating income; protecting against future events
Tax status	• income; capital gains; inheritance taxes; available allowances - investments should be tax efficient
Investment preferences taking into account ethical, religious, and etc.	• This enable CMO determine the best portfolio mix
Risk tolerance	• Risk averse vs Balanced vs Risk taker

3.9.7 Investment Objectives and Strategy

Having collected all the core information needed about the client, the adviser can then turn to agreeing their investment objectives and risk profile. Typical financial objectives include:

- maximizing future growth
- protecting the real value of capital
- generating an essential level of income
- protecting against future events.
- A combination of two or more of the above

3.9.8 Once the client's investment objectives have been agreed, the adviser needs to look at developing an investment strategy that can be used to achieve these objectives. In developing an investment strategy, the adviser will need to take account of the following factors/ considerations:

- Risk profile
- Liquidity requirements
- Time horizons
- Tax status
- Investment preferences.

Investment strategy factor/ considerations	Explanation/ rationale
Risk Profile	**A client's risk profile is made up of a combination of attitudes and risk capacity – that is the client's ability to absorb any financial losses that might arise from making a particular investment. These allow a risk classification or profile to be determined that can be agreed with the client and this is examined further in the next section.**
Liquidity Requirements	**It is also essential to understand a client's liquidity requirements as this will also have a clear impact on the selection and construction of any investments. Liquidity refers to the amount of funds a client might need both in the short and long term. When constructing an investment portfolio, it is essential that an emergency cash reserve is put to one side which the client can access without having to disturb longer-term investments. If there are known liabilities that may arise in future years, consideration should also be given as to how funds will be realized at that time.** **Consideration needs to be given as to whether it is sensible to plan to realize profits from equities as market conditions may be such as to require losses to be established unnecessarily. Instead, conservative standards suggest investing an appropriate amount in bonds that are due to mature near the time needed so that there is certainty of the availability of funds.**

	The lower the client's liquidity requirements and the longer their timescale, the greater will be the choice of assets available to meet the client's investment objective. The need for high liquidity allied to a short timescale demands that the client should invest in lower-risk assets such as cash and short-dated bonds, which offer a potentially lower return than equities; if the opposite is true, the portfolio can be more proportionately weighted towards equities. Whatever their requirements, it is important, however, that the client maintains sufficient liquidity to meet both known commitments and contingencies.
Time Horizons	Time horizon refers to the period over which a client can consider investing their funds. Definitions of time horizons vary, but short term is usually considered to be from one to four years, while medium term refers to a period from five to ten years and long term is considered to be for a period of ten years or more. Time horizon is very relevant when selecting the types of investment that may be suitable for a client. It is generally stated that an investor should only invest in equities if they can do so for a minimum period of five years. This is to make the point that growth from equities comes about from long-term investment and the need to have the time perspective that can allow an investor to ride out periods of market volatility.
Tax Status	Establishing the client's tax position is essential so that their investments can be organized in such a way that the returns attract the least tax possible. This requires the firm to be aware of what taxes may affect the investor, such as taxes on any income arising or on any capital gains, how these are calculated and what allowances may be available. An adviser will also need to establish the client's residence and domicile status as these may impact how any investments are structured.
Investment Preferences	Some investors prefer to either exclude certain areas of the investment spectrum from their portfolios or concentrate solely on a particular investment theme, such as socially responsible investment or the construction of the portfolio in accordance with Islamic principles.

3.9.9 Risk Profile

Firms must ensure that any recommendations they make are both suitable and appropriate. To do so, a firm should ensure that the information it gathers also includes details about:

- a client's knowledge and experience in relation to the investment or service that will be considered for recommendation
- the level of investment risk that the client can bear financially and whether that is consistent with their investment objectives.

3.9.10 Investment always involves a trade-off between risk and return. However, different people are prepared to tolerate different levels of investment risk and investment risk means different things to different investors. Variations in attitude arise because of individual differences in circumstances, experiences, and psychological make-up.

3.9.11 A client's risk profile is made up of three components:

- Risk tolerance – this is the client's willingness to accept a certain level of fluctuation in the value of their investments without feeling an immediate need to sell.
- Attitude to risk – this represents their personal opinion on the risks associated with making an investment based on their prior knowledge and experience.
- Risk capacity – this is the client's ability to absorb any financial losses that might arise from making a particular investment.

3.9.12 Risk Attitudes

Risk attitudes help to identify the degree of uncertainty that an investor can handle with regard to a negative change in the value of their portfolio. These attitudes may be influenced by both objective and subjective factors.

3.9.13 Taken together, these three elements should allow a risk classification or profile to be determined that can be agreed with the client.

3.9.14 The risk assessment process usually starts with investigation of attitudes; consideration of risk capacity usually follows later since it requires knowledge of the client's objectives and the investments that are being considered.

Objective Factors	• The timescale over which a client may be able to invest will determine both what products are suitable and what risk can be adopted. • Family commitments are likely to have a significant impact on a client's risk profile as they will want to meet their obligations, which may make higher-risk investments less suitable. • Wealth will clearly be an important influence on the risk that can be assumed. A client with few assets can little afford to lose them, while ones whose immediate financial priorities are covered may be able to accept greater risk. • Stage of life is equally important as it will impact the level of risk that can be adopted and the time horizon over which the client invests. • The age of the client will often be used in conjunction with the above • factors to determine acceptable levels of risk.
Subjective Factors	• Investors who are more knowledgeable about financial matters are more willing to accept investment risk. • Some individuals have a psychological make-up that enables them to take risks more freely than others and see such risks as an opportunity. • A client's preferred investment choice such as a client's normal preferences for the relative safety of a bank account versus the potential risk of stocks and shares. • A client's approach to bad decisions. Some clients can take the view that they assessed the opportunity fully and therefore any loss is just a cost of investing. Others regret their wrong decisions and therefore avoid • similar scenarios in the future.

3.9.14.1 Establishing objective factors is clearly a preferable and more accurate way to help define a client's risk tolerance, but subjective factors clearly have a part to play. Subjective factors allow an adviser to try and establish a client's attitude to taking risks.

3.9.14.2 A client's attitudes and experiences must also play a large part in the decision-making process. A client may well be financially able to invest in higher-risk products and these may well suit their needs, but if they are by nature cautious, they may well find the uncertainties of holding volatile investments unsettling, and both the firm and the client may have to accept that lower-risk investments and returns must be selected.

3.9.15 Risk Capacity

3.9.15.1 Risk capacity is the client's ability to absorb any losses that may arise from making a particular investment.

3.9.15.2 Risk tolerance and risk perception are partly subjective, but risk capacity is a matter of fact. While subjective factors largely determine risk perception and attitude, the key question in assessing risk capacity is more what would be the consequences for the client if losses were incurred.

3.9.15.3 In some cases, risk capacity will play the most important role in determining the client's overall risk profile. The client's capacity for risk will also be affected by the level of investment being considered. If the amount at risk represents a significant portion of the overall portfolio, risk capacity may be diminished. Risk capacity will be greater when the amount at risk is a small fraction of available capital.

3.9.16 Suitability

3.9.16.1 Once having gathered sufficient information about the customer, the steps expected of a firm to ensure its recommendations are suitable and appropriate for the client will vary depending upon the needs and priorities of the customer, the types of investment or service being offered and the nature of the relationship between the firm and the customer.

3.9.16.2 In general terms, the process that is involved can be broken down into a series of steps that include:

- agreeing the client's investment objectives
- investigating and agreeing the client's attitudes to risk and risk capacity
- analyzing the client's financial situation and synthesizing this information to create understandable summaries of the client's financial position, asset allocation and cash flow
- from this analysis, identifying the key areas that need action recognizing that many clients have multiple objectives and may have different risk attitudes for each
- determining the best investments, solutions, or combinations of both that meet the client's needs and are suitable for their purposes.

3.9.16.3 When considering whether a particular investment is suitable, it is necessary to look at the features of the recommended investment including:

- its terms and conditions
- its flexibility
- the inherent risks including asset allocation and structural risks such as counterparty risk
- the term or duration of the investment
- the expected return
- the charges applied by the product provider.

3.9.16.4 This involves going beyond a product's description to analyze its underlying components and characteristics.

3.9.16.5 When a firm proposes to offer investment advisory services or discretionary portfolio management, it should first assess whether such services are suitable for the client. If the firm intends to offer other investment services, e.g., trading futures and options or more exotic investments, then it should go further and ensure that they are not just suitable but also appropriate for the client's financial position and their attitude to risk.

3.9.16.6 In assessing whether the investment services are suitable for the client, the firm should gather information on:

- the client's knowledge and experience
- the types of services and transactions with which the client is familiar
- the nature, volume, frequency, and time that the client has been involved in such services and transactions
- the client's level of education, profession, or relevant former profession.

3.9.16.7 The general principle behind this is that the firm must take reasonable steps to ensure it makes no recommendation to a customer unless it is suitable for that customer and that the client understand the risks involved. Suitability will have regard to the facts disclosed by the customer and other facts that the firm should reasonably be aware of.

3.9.16.8 If the firm determines after assessment that the service or product is not appropriate for the client, then it should issue a risk warning to the client. If the client still wishes to proceed despite the warning, then it is up to the firm to decide whether it will do so.

3.9.16.9 If the firm is acting as investment manager for a client, there is an ongoing requirement that it must ensure that the portfolio remains suitable. Equally, if a customer has agreed to the firm pooling his or her funds with others, the firm must take reasonable

3.9.17 Providing Recommendations: Suitability Reports

3.9.17.1 Having assessed what services and products are suitable and appropriate, the firm should provide the client with a report which should set out, among other things, why the firm has concluded that a recommended transaction is suitable for the client.

3.9.17.2 A key regulatory principle is that a market intermediary is required to give sufficient information to the client to ensure that the client's decisions are informed. This requires a market intermediary to provide all explanations to the client in writing and retain a copy of the explanation in the client's file if the explanation was given to the client orally. The market intermediary should also document any opinion that an explanation is not required due to a client's existing knowledge. A copy of this information should be retained for record purposes.

3.9.17.3 Clear documentation directed at the client personally such as a 'reason why' letter or a suitability report can be a useful means of demonstrating that the recommendation was suitable for the consumer. Suitability reports serve two purposes:

- meet regulatory standards that require the CMO communications to be fair, clear, and not misleading;

- They also need to be understandable to the client and provide a clear summary of their objectives, needs, priorities and relevant existing investments, demonstrating how the adviser has taken account of these.

3.9.17.4 Firms should consider whether their suitability report:

- is tailored to the client and uses clear and plain language
- explains the reasons for all recommendations and how they relate to the client's objectives
- provides a balanced view and highlights the risks associated with the recommendations
- explains the costs, charges and potential penalties attached to the recommendations
- identifies why the selected investments are suitable to meet the client's needs and objectives.
- Maked provision for an acknowledgement from the client that they have understood the suitability report

3.9.18 Contents of a suitability report

The contents of the suitability report should be used as a means for the CMO to demonstrate that it has applied the principles for conduct risk management and has communicated to the clients and obtained affirmation of their clients that they have understood and accepted the investment proposal made to them. A suitability report should contain the following:

1) Introduction or executive summary
2) Details of the licensed Dealer/ Investment Adviser/ CMO
   - the name
   - contact details
   - License details, including license number
3) Details of licensed representative acting on behalf of the CMO
   - the name
   - contact details
   - License details, including license number
   - a statement that the representative has been authorized to act on behalf of the CMO
4) Details of the advice provided
   - a statement setting out the advice
   - Investment vehicle
   - Investment strategy
   - Charge analysis (Current vs proposed) Asset classes
   - Alternative's solutions and reasons why not recommended
   - Portfolio Mix where relevant

5) Basis on which advise provided:
   - Summary of current situation (summarizes Informa from KYC)
   - Investment preferences
   - Investment Knowledge
   - Risk profile
   - Current investment profile

- Review of existing investments and discussion of proposed changes

- information about the basis on which the advice is or was given

6) Fees and charges, other benefits to service provider:
   - information about the remuneration, commission and other benefits accruing to service provide (and the other related or associated persons)
   - Includes future revenues from "tailing fees"
   - Includes referral fees payable to the entity for recommending the products
   - details of any interests, associations or relationships that might reasonably be expected to be, or to have been capable of, influencing the providing entity in providing the advice.

7) Risk warnings
   - Risks pertaining to recommended product
   - Risk arising if advice is based on incomplete or inaccurate information
   - Risks arising from switching advice
   - Details of when to contact the adviser for a change in circumstances which may result in a change in the suitability assessment

8) Client acknowledgement that they have read and understood the contents of the Suitability report

Appendices & attachments that provide more information e.g., reviews and other analysis

3.9.18.1 Suitability reviews should be undertaken at least once a year. However, the frequency of this assessment shall be increased depending on the characteristics of the customer, such as the risk tolerance, and the nature of the recommended insurance-based investment product.

3.10 Communicating to clients about their investments

3.10.1 As noted above communication with clients is a key component of the investment advisory process. Once clients have made the investment decision, CMOs continue to communicate to the client concerning their investments. This should include ensuring the following:

(1) Delivery of Contract Notes for all transactions effected for and on behalf of the client. See Section 85 of the Securities Act which prescribes the following contents:

Section 85 (2) of the Securities Act

A contract note shall include—

(a) the name or style under which the dealer carries on business and the address of the principal place at which it carries on the business;
(b) where the dealer is acting as principal, a statement that it is so acting;
(c) the name of the person, if any, to whom the dealer is required to give the contract note;
(d) the date of the contract and the date on which the contract note is made out;
(e) the quantity and description of the securities which are the subject of the contract;

(f) except in the case of a securities exchange, the price per unit of the securities;
(g) the amount of consideration payable under the contract or, in the case of a transfer of an interest in securities, sufficient particulars of the securities transferred;
(h) the rate or amount if any, payable in respect of the contract;
(i) the date of settlement; and
(j) such other information as may be prescribed by regulations made in accordance with this Act, to ensure a complete audit trail for the execution of customer instructions and settlement of securities transactions.

(2) Provision/ Delivery of statements showing the clients investments as at a report date. Statements should also be available on demand and should be free of charge. The format of the customer statements is prescribed in the Securities (Accounting and Financial Requirements) Rules.

Rule 20 - Confirmation and periodic information

(2) Where a licensee effects a sale or purchase of securities with or for a customer, he shall ensure that the customer is sent with due dispatch a contract note containing the essential details of the transaction in accordance with section forty-one of the Act
(3) (2) Where a licensee acts as an investment manager for a customer, he shall ensure that the customer is sent at suitable intervals a report stating the value of the portfolio or account at the beginning and end of the period, its composition at the end and, in the case of a discretionary portfolio or account, changes in its composition between those dates.

CMOs should consider providing a statement of holdings at least once every month.

(3) Ensuring customer orders are prioritized over the CMOs own orders

Rule 21 - Customer order priority

A licensee shall deal with customer and own account orders fairly and in due turn.

(4) Ensuring timely execution of customer orders, redemptions, and other client transactions

Rule 22 - Timely execution

When a licensee has agreed or decided in his discretion to effect or arrange a customer order, he shall affect or arrange the execution of the order as soon as is reasonably practicable in the circumstances.

Timely execution also applies to other products such as Collective Investment Schemes where there is an expectation that buying and selling of CIS units will be executed timely.

(5) Ensure best execution of client orders

Rule 23 – Best execution

Where a licensee deals with or for a customer, he shall take all reasonable steps to find and deal on the terms which are the best available to the customer.

(6) Ensure prompt allocation of transactions

Rule 24 - Timely allocation

A licensee shall ensure that a transaction he executes is promptly allocated.

(7) Ensure fair allocation of customer orders

Rule 25 - Timely allocation

Where a licensee has aggregated an order for a customer transaction with an order for an own account transaction, or with an order for another customer transaction, then in the subsequent allocation-

(a) he shall not give unfair preference to himself or to any of those for whom he dealt; and
(b) if all orders cannot be satisfied, he shall give priority to satisfying orders for customer transactions.

(8) Ensure Investors assets/ investments are safeguarded

Rule 29 - Safeguarding of customer investment

A licensee who has custody of a customer's securities in connection with or with a view to securities business shall-

(a) keep safe, or arrange for the safekeeping of, any documents of title, or documents evidencing title, relating to them; and
(b) ensure that any securities that he buys or holds for a customer are properly registered in his name or, with the consent of the customer, in the name of an appropriate nominee.

Rule 29(b) above requires the CMO to ensure that it does not comingle its clients' assets with those of the CMO and/ or other clients. The accounting and financial requirements rules provide further guidance on how client money should be accounted for if kept in an omnibus account.

3.11 Prevention of market Malpractices

3.11.1 The Securities Act and the Conduct of Business Rules prescribe certain market practices as illegal See full list below). CMOs should therefore put in place policies and procedures to ensure that the firm and its staff do not engage in any malpractices. Malpractices therefore pose both a conduct risk as well as a legal and regulatory risk as a breach of the above provisions could not only result in unfair outcomes for clients but represents undesired conduct which results in revocation/ cancellation of the CMO's license.

3.11.2 The following are some of the malpractices specified in the Act and the rules:

1) **Short selling:** Under Section 87 of the Act is prohibited.
"A person who short-sells securities at or through a securities exchange, commits an offence, unless at the time of the sale—
(a) the person or the person's principal has a presently exercisable and unconditional right to vest the securities in the purchaser of the securities;

(b) the person or that person's principal has deposited, in the manner prescribed, one hundred percent collateral against the short sale, marked to market at the close of every trading day until the transaction is complete;
(c) the person or that person's principal owns another security convertible into the securities sold or an option or right to acquire the securities sold and, within ten days after the sale, exercises the conversion privilege, option or right and delivers the security, so acquired, to the purchaser or transfers the convertible security, option or right to the purchaser of the security: or
(d) the person has entered into a fully secured and unconditional borrowing agreement or arrangement pursuant to which that person shall be able to deliver the securities for settlement in accordance with the rules of the relevant securities exchange.

The example below illustrate how short selling can harm investors especially if an element of market manipulation through release of false information designed to solicit a market response that favors the short sellers' position.

GameStop

Short sellers betting against mall retailer GameStop have lost $5.05 billion mark-to-market in 2021, according to a note published yesterday by S3 Partners when the stock was 16% higher in intraday trading.1 Up over 600% since the start of the year on a surge of retail investor interest and resulting short squeezes, GameStop closed up 93% yesterday and is set to continue its mind-bending run higher today.

One of the biggest GameStop short seller "victims" is Melvin Capital, a hedge fund that started the year with $12.5 billion in AUM and lost almost 30% through Friday last week, according to The Wall Street Journal.2 It announced an emergency infusion of $2.75 billion from fellow hedge funds Citadel and Point72 on Jan. 25 and told CNBC today that it closed out its short position in GameStop on Tuesday afternoon.

Shares in other Melvin shorts like German drugmaker Evotec, German battery maker Varta, and Polish video game firm CD Project are also rising this week. Traders Reuters spoke with said this was "likely linked to Melvin Capital closing out its shorts following losses on GameStop and other investments." Meanwhile, Citron Research just revealed it covered most of its GameStop short position "in the $90s at a loss 100%."

Source: https://www.investopedia.com/short-sellers-lose-usd5-05-billion-in-bet-against-gamestop-5097616

2) Front running (Rule 26 of the Conduct of Business Rules)

Where a licensee intends to publish to customers a price-sensitive recommendation or research or analysis, he shall not knowingly affect an own account transaction in the investment concerned or in any related investment until the customers for whom the publication was principally intended have had, or are likely to have had, a reasonable opportunity to react to it.

3) Churning (Rule 27 of the Conduct of Business Rules)

A licensee shall not-

(a) deal or arrange a deal in the exercise or discretion for any customer; or

(b) advise a customer to deal,

(c) if the dealing could in the circumstances reasonably be regarded as too frequent or too large.

4) Insider dealing (Rule 28 of the Conduct of Business Rules)

A licensee shall not knowingly profit or seek to profit, either for his own account, the account of a customer or any third party, from inside information in the hands of any of his officers, employees, or agents, or assist anyone with such information to make a profit for himself.

3.11.3 Specific controls the CMOs can deploy to mitigate against market malpractices include the following:

(1) Instituting Clients complaints procedures (Rule 30) and Guidance Note No. 1 of 2017, Minimum complaints handling procedures for Capital markets licensees in Zambia

(2) Instituting anonymous hotlines/ whistle blowing procedures for both clients and staff

(3) Ensuring adequate supervision of Staff (Refer to Rule 32 of the Conduct of Business Rules

(4) Ensuring they institute adequate compliance measures (Rule 31)

(5) Inclusion of breaches of these offences and taking enforcement actions against employees and officers involved in the breaches.

SECTION 4: OPERATIONAL RISK

4.1 Definition of Operational Risk

4.1.1 Operational risk arises from potential problems and/or loss due to inadequate or failed internal processes, people, and systems, or from external events (The Basel Committee on Banking Supervision). Operational risk sometimes manifests in seemingly insignificant failures that once not addressed result an environment in there is an increased possibility of significant loss to the CMO and its clients.

4.1.2 The table below provides examples of operational risks that could arise categorized in line with the above definition:

Source of Operational Risk	Examples of operational risks (Source: The Joint Forum of banking, securities, and insurance supervisors and www.sweetprocess.com)
People	• Fraud • Loss or lack of key personnel • Unauthorized activity • Inadequate training and supervision • Inadequate staffing levels
Internal Processes	• Errors in valuation or pricing models and processes • Payment or settlement failures • Inadequate or insufficient documentation and record keeping • Internal or external reporting • Project management failures
Systems	• Failures during the development and systems implementation process • Failures of the system itself • Inadequate resources
External Events	• External crime • Outsourcing and insourcing risk • Natural and other disasters • Regulatory risk • Political risk • Utilities failures • Competition

4.2 Drivers of Operational Risk

4.2.1 The main drivers of operational risk can be deduced from the definition of operational risk provided above. The following are the drivers:

1) **People**: People play a critical role in any CMO's operations and are at the core of most of the organization's processes. It is therefore important that measures are put in place to ensure that a CMO's employees (people) are adequately trained to perform various tasks assigned to them and that they uphold the highest t levels of integrity, professionalism, due competence, and care at all times. This relates to both full-time staff and any others e.g., consultants, outsourced staff, part time staff etc.
2) **Internal Processes:** Weak, ineffective, and inefficient processes increase the likelihood of operational risk crystallizing.
3) **Systems:** In an increasingly digitized world, the significant role of systems within the operational process has never been more important. Well-functioning systems are essential in reducing operational risk.
4) **External Events:** Despite these being outside the control of CMOs, their effects could still negatively impact the CMO's operations. It is therefore expected that CMOs put in place contingency plans that can be deployed in the instance of such events.

4.3 Practical steps and guidance for the CMOs on managing the particular risk

4.3.1 People:

- Establish employee training manuals that will guide on aspects related to assess and evaluating employees' skills adequacy, skills gaps within the CMO and training needs.
- Ensure that codes of ethics are in place for all CMO staff.
- Ensuring adequate staffing levels within the CMO

4.3.2 Internal Processes:

- Ensure the existence of documented procedures and controls are in place.
    - Identify significant business process and activities
    - Document these processes and activities/controls
    - Identify and assign roles and responsibilities
    - Periodic reviews/updates of the policies and procedures manuals
- Ensure controls are in place to help avoid internal process failures. These include maker checker mechanisms, review, and sign off procedures etc.
- Adequate and up to date record keeping is in place.

4.3.3 Systems:

- CMOs must ensure to put in place systems such as accounting systems, brokerage systems, asset management systems, custody systems, credit rating systems as appropriate
- The use of excel is strongly discouraged
- CMOs must strive for automation of most tasks to minimize risks arising from human failure or error.
- CMOs must have appropriate measures to ensure systems are protected from unauthorized use this includes putting in place physical access restriction for any highly sensitive areas, logical access controls etc. In addition, CMOs must ensure that they have standard laid out procedures guiding on processes to be followed in the event of cyberbreaches for example

issuance of alerts to clients, ask users to immediately logout or change password, and report suspicious transactions.

- CMOs, particularly those heavily reliant on technology, must ensure they put in place adequate measures to mitigate against cyber related risks (e.g., spyware and ransomware attacks, data breaches etc.) examples of these measures include the use of firewalls.
- CMOs to put in place measures to mitigate against system down and ensure availability of core systems for example Network Redundancies.
- The CMO must ensure measures are put in place to ensure integrity and security of data and uphold the utmost confidentiality.
- Mechanisms must be in place to detect and address any system failures or errors.
- In all event of system failures, CMOs must ensure that the regulator, clients, and other stakeholders are immediately notified of any hardware or system failures. This should include an explanation of the causes and the actions being taken by the CMO to resolve the matter. CMOs must indicate when they expect to resolve the problem and must provide the contact details where queries can be addressed.
- If there is a security breach on the CMO's systems, the CMO must ensure that the regulator, clients, and other stakeholders are immediately notified. The notification to clients should contain specific instructions of what they should do to safeguard their data e.g., immediately change passwords, notify the CMO of any suspicious transactions etc.

4.3.4 External Events:

- The CMO must ensure that a robust business continuity plan must be in place. This must include disaster recovery plan. In addition, the CMO must effectively utilities, where possible, insurance in mitigating the loss from unforeseen external events e.g., insuring equipment, property etc. against accidents or fires.

4.4 Role of Oversight Functions in managing Operational Risk

4.4.1 The Risk Management Function must ensure that operational risks are adequately identified, assessed, and mitigated. In addition, the risk management function must ensure that adequate controls are put in place to minimize operational risk.

4.4.2 The Compliance Function must ensure that the CMO's operational environment is following the requirements of any prescribed regulatory standards. If this is done, operational risks may be minimized.

4.4.3 The Internal Audit function must ensure that they assess the effectiveness of systems and procedures that have been put in place to mitigate operational risk and recommend ways in which these can be improved if weaknesses have been identified.

4.5 Role of Senior Management (SM)

4.5.1 The CMO's senior management are expected to ensure that adequate measures, including policies and procedures are put in place to help minimize operational risks. Senior management must also ensure that adequate controls are in place to ensure that policies and procedures are not only being implemented, but that they are also being implemented correctly.

4.5.2 Senior management must also establish robust processes for monitoring effectiveness of internal controls to address operation risk.

Case study:

A Fund manager for a Collective Investment Scheme could not meet its reporting obligations to the Commission including

- Submission of Monthly custody returns
- Submission of Quarterly returns
- Submission of accurate statements to investors
- Failure to finalize audits and produce audited financial statements

This resulted in the following failures

- 90% of assets were not taken into custody posing a risk of loss to investors
- Inaccurate unit prices, resulting in overvaluation of redemptions and erosion of the fund size for remaining investors (Fund Insolvency)
- Inaccurate customer statements were circulated to clients which could not be aligned to information contained in the Asset management system and financial records. In some instances, clients complained that contributions made by them were not reflected on their statement. Suffice to mention that client statements were only produced for selected clients following threats of "We shall seek the intervention of the regulator." In some instances, statements were amended or corrected without any explanation to investors
  - Some customers were wrongly advised to invest in the CIS believing they were investing in a fixed term deposit

The above was because of the following operational failures

- No prescribed procedures for valuation of assets. Staff relied on a system valuation which they did not understand. It turned out there was a glitch in the software which resulted in over-valuation of redemption prices
- Lack of supervision by Senior Management
- lack of training for staff in the operation of the fund management system in use
- Lack of product understanding by the system developer who in turn developed the wrong system for their client
- Lack of adequate qualifications of the staff involved in the accounting and investment functions. The accountants lacked the requisite knowledge for accounting for a CIS
- Use of unlicensed representatives E.g., the Fund Managers allowed a receptionist without a representative license to market the company's product and the person advised clients to invest in CIS as fixed term deposits which would pay back three times the amount invested. This was based on conversations she had overheard from advisers within the office. Management did fail to ensure that there was compliance with laid down procedures before accepting the funds from the client and hence there was no scrutiny of the information provided to its clients when finalizing the investment.

- The broker allows an unlicensed dealer to travel on behalf of a client with a license. Assignment of wrong and/or duplicate client numbers

4.6 Role of Board of Directors

4.6.1 The CMO's Board of Directors must, primarily through its Risk and Audit Committee, monitor the efficiency of the Company´s internal control, internal audit (if applicable), and risk management

Examples
Receive and review reports from the risk management function, compliance function and internal audit and ensure to take corrective action

systems. To do this, the Board must guarantee it is receiving adequate information regarding all of these areas and that it makes sure any identified weaknesses are addressed appropriately and in a timely manner.

SECTION 5: CONSIDERATIONS FOR OPERATIONAL RISK ARISING FROM INFORMATION AND COMMUNICATION TECHNOLOGY ("ICT")

5.1 Introduction

5.1.1 The purpose of Information and Communication Technology risk management is to assist institutions to establish an effective mechanism that can identify, measure, monitor, and control the risks inherent in institutions' ICT systems, ensure data integrity, availability, confidentiality, and consistency and provide the relevant early warning mechanism.

5.2 Board and Senior Management Oversight

5.2.1 Specific Responsibilities for the Board of Directors

The board of directors of institutions has the following responsibilities with respect to the management of information and communication technology risk:

- Ensure that the institution has in place an appropriate ICT governance structure and risk management framework which suits its own circumstances, business needs and risk tolerance.
- Periodically review the alignment of ICT strategy with the overall business strategies and significant policies of the institution.
- Approve ICT risk management strategies and policies.
- Set high ethical and integrity standards and establish a culture within the institution that emphasizes and demonstrates to all levels of personnel the importance of ICT risk management.
- Establish an ICT steering committee which consists of representatives from senior management, the ICT function, and major business units, to oversee these responsibilities and report the effectiveness of strategic ICT planning, the ICT budget and actual expenditure, and the overall ICT performance to the board of directors and senior management periodically.
- Ensure that an effective internal audit of the ICT risk management is carried out by operationally independent, well-trained, and qualified staff, which report should be submitted to the audit committee; and
- Ensure the appropriation of funding necessary for ICT risk management function.
- Understand the major ICT risks inherent in the institution's business, setting acceptable levels for these risks, and ensuring the implementation of the measures necessary to identify, measure, monitor and control these risks.

5.3 Specific Responsibilities for the Senior Management

5.3.1 The following are key responsibilities of senior management with regards to ICT risk: -

- Ensuring that all employees of the institution fully understand and adhere to the ICT risk management policies and procedures approved by the board of directors and the senior management and are provided with pertinent training.
- Ensuring customer information, financial information, product information and core CMO system of the legal entity are held in a secure environment.
- Reporting in a timely manner to the CBK any significant adverse incidents of information and communication systems or unexpected events, and how they have been handled;
- Cooperating with the CBK in the surveillance of the risk management of information systems, and ensure that supervisory opinions are followed up; and
- Performing other related ICT risk management tasks.

5.4 Head of Information and Communication Technology

5.4.1 The following are the responsibilities of the Head of ICT:

- Play a direct role in key decisions for the business development involving the use of ICT in the institution;
- Ensure that information systems meet the needs of the institution, and the ICT strategies, in particular information system development strategies, comply with the overall business strategies and ICT risk management policies of the institution;
- Be responsible for the establishment of an effective and efficient ICT organization to carry out the ICT functions of the institution. These include the IT budget and expenditure, IT risk management, ICT policies, standards and procedures, ICT internal controls, professional development, ICT project initiatives, ICT project management, information system maintenance and upgrade, ICT operations, ICT infrastructure, Information security, disaster recovery plan (DRP), ICT outsourcing, and information system retirement;
- Ensure the effectiveness of ICT risk management throughout the organization including all branches.
- Organize professional trainings to improve technical proficiency of staff.

5.4.2 Staffing of the Information and Communication Technology Unit:

Institutions should designate qualified officer(s) in the Management function for ICT management. Staff in each position should meet acceptable minimum requirements on professional skills and knowledge. The following risk mitigation measures should be incorporated in the selection and management of ICT staff:

- Verification of personal information including confirmation of personal identification issued by government, academic credentials, prior work experience, professional qualifications, certificates of good conduct by the Police;
- Ensuring that ICT staff meet professional ethics and integrity by obtaining character reference from independent referees, former employers, relevant sector regulators;
- Signing of agreements with employees about understanding of ICT policies and guidelines, non-disclosure of confidential information, authorized use of information systems, and adherence to ICT policies and procedures; and
- Evaluation of the risk of losing key ICT personnel, especially during major ICT development stage or in a period of unstable ICT operations, and the relevant risk mitigation measures such as staff backup arrangement and staff succession plan.

5.4.3 Intellectual Proprietary Rights

Institutions should put in place policies and procedures to:

- ensure the utilization of only genuine and licensed software to avoid the violation of the law regarding intellectual properties,
- ensure purchase of legitimate software and hardware,
- prevention of the use of pirated software, and
- the protection of the proprietary rights of ICT products developed by the institution and ensure that these are fully understood and complied with by all employees.

5.5 ICT Risk Management Framework

5.5.1 Information and Communication Technology Strategy

Institutions should formulate an ICT strategy that aligns with the overall business plan of the institution, ICT risk assessment plan and an ICT operational plan. The ICT strategy should ensure that adequate financial resources and human resources are allocated to maintain a stable and secure ICT environment.

5.5.2 ICT Risk Management Policy

Institutions should put in place a comprehensive set of ICT risk management policies that include the following areas:

- Information security classification policy,
- System development, testing, and maintenance policy,
- ICT operation and maintenance policy,
- Access control policy,
- Physical security policy,

- Change controls policy,
- Personnel security policy, and
- Business Continuity Planning and Crisis and Emergency Management procedure.

5.5.3 ICT Risk Identification

Risk identification entails the determination of all kinds of threats, vulnerabilities and exposures present in the ICT system configuration which is made up of components such as internal and external networks, hardware, software, applications, systems interfaces, operations, and human elements.

1.1.1.1 Security threats such as those manifested in denial-of-service attacks, internal sabotage and malware infestation could cause severe disruption to the operations of an institution with consequential losses for all parties affected. Vigilant monitoring of these mutating, growing risks is a crucial step in the risk containment exercise.

1.1.1.2 Both threat-sources and threats must be identified. Threats should include the threat- source to ensure accurate assessment. Some common threat-sources include:

- Natural Threats—floods, earthquakes, hurricanes.
- Human Threats—threats caused by human beings, including both deliberate actions (network-based attacks, virus infection, unauthorized access), and unintentional (Inadvertent data entry errors).
- Environmental Threats—power failure, pollution, chemicals, water damage
- The risk management function in the institution should compile a list of threats that are present across the institution and use this list as the basis for all risk management activities.

5.5.4 Identifying Vulnerabilities

1.1.1.3 Different risk management schemes offer different methodologies for identifying vulnerabilities. In general, institutions should start with commonly available vulnerability lists or control areas.

1.1.1.4 The following tools and techniques are typically used to evaluate the effectiveness of controls, and can also be used to identify vulnerabilities:

- Vulnerability Scanners – software that can examine an operating system, network application or code for known flaws by comparing the system (or system responses to known stimuli) to a database of flaw signatures.
- Penetration Testing – an attempt by human security analysts to exercise threats against the system. This includes operational vulnerabilities, such as social engineering.
- Operational and Management Controls – A review of operational and management controls by comparing the current documentation to best practices (such as ISO 17799) and by comparing actual practices against current documented processes.

5.6 Risk Assessment, Measurement and Monitoring

5.6.1 Risk Assessment

1.1.1.5 To determine the likelihood of a future adverse event, threats to an ICT system must be analyzed in conjunction with the potential vulnerabilities and the controls in place for the ICT system. Impact refers to the magnitude of harm that could be caused by a threat's exercise of vulnerability. The level of impact is governed by the potential mission impacts and in turn produces a relative value for the ICT assets and resources affected (e.g., the criticality and sensitivity of the ICT system components and data).

1.1.1.6 A typical risk assessment methodology encompasses the following nine primary steps;

- System Characterization.
- Threat Identification.
- Vulnerability Identification.
- Control Analysis.
- Likelihood Determination.
- Impact Analysis.
- Risk Determination.
- Control Recommendations.
- Results Documentation.

5.6.2 Risk Measurement

1.1.1.7 Institutions should put in place a set of ongoing risk measurement and monitoring mechanisms, which should include:

- Pre- and post-implementation review of ICT projects;
- Benchmarks for periodic review of system performance;
- Reports of incidents and complaints about ICT services;
- Reports of internal audit, external audit, and issues identified by CBK;
- Arrangement with vendors and business units for periodic review of service level agreements (SLAs);
- The possible impact of new development of technology and new threats to software deployed;
- Timely review of operational risk and management controls in operation area;
- Assessment of the risk profile on IT outsourcing projects periodically.

5.6.3 ICT Risk Mitigation

1.1.1.8 Risk mitigation involves prioritizing, evaluating, and implementing the appropriate risk- reducing controls recommended from the risk assessment process.

1.1.1.9 Because the elimination of all risk is usually impractical, it is the responsibility of senior management and functional and business managers to use the least-cost approach and implement the most appropriate controls to decrease mission risk to an acceptable level, with minimal adverse impact on the institution's resources and mission.

1.1.1.10 Generally, risk mitigation can be achieved through any of the following risk mitigation options: -

- Risk assumption - accept the potential risk and continue operating the ICT system or to implement controls to lower the risk to an acceptable level.
- Risk avoidance - avoid the risk by eliminating the risk cause and/or consequence (e.g., forgo certain functions of the system or shut down the system when risks are identified).
- Risk limitation – limit the risk by implementing controls that minimize the adverse impact of a threat's exercising a vulnerability (e.g., use of supporting, preventive, detective controls).
- Risk planning - manage risk by developing a risk mitigation plan that prioritizes, implements, and maintains controls.
- Research and acknowledgment - lower the risk of loss by acknowledging the vulnerability or flaw and researching controls to correct the vulnerability.
- Risk transference - transfer the risk by using other options to compensate for the loss, such as purchasing insurance.

1.1.1.11 Institutions should therefore implement a comprehensive set of risk mitigation measures complying with the ICT risk management policies and commensurate with the risk assessment of the institution. At a minimum, the mitigation measures should include:

- A set of clearly documented ICT risk policies, technical standards, and operational procedures, which should be communicated to the staff frequently and kept up to date in a timely manner;
- Areas of potential conflicts of interest should be identified, minimized, and subject to careful, independent monitoring. Also, it requires that an appropriate control structure is set up to facilitate checks and balances, with control activities defined at every business level, which should include:
  - (i) Top level reviews;
  - (ii) Controls over physical and logical access to data and system;

(iii) Access granted on “need to know” and “minimum authorization” basis;

(iv) A system of approvals and authorizations; and

(v) A system of verification and reconciliation.

5.7 Information Security

1.1.1.12 Institutions should put in place an information and communication security management function to develop and maintain an ongoing information security management program. The core objective of the Information and communication security management program must be premised around ensuring confidentiality, integrity, and availability of data. The Information and communication security management program must include;

- Promoting information security awareness,
- advising other ICT functions on security issues,
- serve as the leader of ICT incident response team, and
- report the evaluation of the information security of the institution to the board periodically.

1.1.1.13 The Information and communication security management program should be documented in an information and communication security policy which should also document the information security standards, strategy, implementation plan, and an ongoing maintenance plan.

1.1.1.14 The information security policy should include the following areas:

- ICT security policy management,
- Organization information security,
- Asset management,
- Personnel security,
- Physical and environment security,
- Communication and operation security,
- Access control and authentication,
- Acquirement, development, and maintenance of information system,
- Information security event management,
- Business continuity management, and
- Compliance.

5.7.1 Information Confidentiality

1.1.1.15 The Information and Communication Technology function of institutions should oversee the establishment of an information classification and protection scheme. All employees of the institution should be made aware of the importance of ensuring information confidentiality and provided with the necessary training to fully understand the information protection procedures within their responsibilities.

5.7.2 Authentication and Access Control

1.1.1.16 Institutions should have an effective process to manage user authentication and access control. Access to data and system should be strictly limited to authorized individuals whose identity is clearly established, and their activities in the information systems should be limited to the minimum required for their legitimate business use. An appropriate user authentication mechanism commensurate with the classification of information to be accessed should be adopted.

1.1.1.17 Timely review and removal of user identity from the system should be implemented when a user transfers to a new job or leaves the institution. The following controls should be put in place: -

(i) Physical Security Zones

Institutions should ensure all physical security zones, such as computer centers or data centers, network closets, areas containing confidential information or critical ICT equipment, and respective accountabilities are clearly defined, and appropriate preventive, detective, and curative control measures are put in place.

(ii) Logical Security Domains

Institutions should divide their networks into logical security domains (hereinafter referred to as the "domain") with different levels of security. The following security factors must be assessed in order to define and implement effective security controls, such as physical or logical segregation of network, network filtering, logical access control, traffic encryption, network monitoring, activity log, for each domain and the whole network:

- Criticality of the applications and user groups within the domain;
- Access points to the domain through various communication channels;
- Network protocols and ports used by the applications and network equipment deployed within the domain;
- Performance requirement or benchmark;
- Nature of the domain, i.e., production or testing, internal or external;
- Connectivity between various domains; and
- Trustworthiness of the domain.

5.8 Operating System and System Software

5.8.1 Institutions should secure the operating system and system software of all computer systems by:

- Developing baseline security requirement for each operating system and ensuring all systems meet the baseline security requirement;
- Clearly defining a set of access privileges for different groups of users, namely, end-users, system development staff, computer operators, and system administrators and user administrators;
- Setting up a system of approval, verification, and monitoring procedures for using the highest privileged system accounts;
- Requiring technical staff to review available security patches, and report exceptions in the patch status to Head of ICT periodically; and
- Requiring technical staff to include important items such as unsuccessful logins, access to critical system files, and changes made to user accounts in system logs monitor the systems for any abnormal event manually or automatically and report the monitoring periodically.

5.9 Application Software

5.9.1 Institutions should ensure the security of all the application software by:

- Clearly defining the roles and responsibilities of end-users and IT staff regarding the application security;
- Implementing a robust authentication method commensurate with the criticality and sensitivity of the application system;
- Enforcing segregation of duties and dual control over critical or sensitive functions;
- Requiring verification of input or reconciliation of output at critical junctures;
- Requiring that the input and output of confidential information be handled in a secure manner to prevent theft, tampering, intentional leakage, or inadvertent leakage;
- Ensuring the system can handle exceptions in a predefined way and provide meaningful messages to users when the system is forced to terminate; and
- Maintaining audit trail in either paper or electronic format.
- Requiring the user administrator to monitor and review unsuccessful logins and changes to user's accounts.

5.10 Audit Trail

5.10.1 Institutions should have a set of policies and procedures controlling the logging of activities in all production systems to support effective auditing, security forensic analysis, and fraud

prevention. Logging can be implemented in different layers of software and on different computer and networking equipment, which falls into two broad categories:

- Transaction journals are generated by application software and database management system, and contain authentication attempts, modification to data and error messages. Transaction journals should be kept according to the information retention policy legally stipulated in the country.
- System logs are generated by operating systems, database management system, firewalls, intrusion detection systems, and routers, etc. and contain authentication attempts, system events, network events and error messages. System logs should be kept for a period proportionate to the risk classification, but not less than one year.
- Institutions should ensure that sufficient items are captured in the logs to facilitate effective internal controls, system trouble shooting, and auditing while taking appropriate measures to ensure time synchronization on all logs. Sufficient disk space should be allocated to prevent logs from being overwritten. System logs should be reviewed for any exception. The review frequency and retention period for transaction logs or database logs should be determined jointly by ICT function and pertinent business lines and approved by the IT Steering Committee.

5.11 Encryption Technologies

5.11.1 Institutions should have the capacity to employ encryption technologies to mitigate the risk of losing confidential information in the information and communication systems or during its transmission. Appropriate management processes of the encryption facilities should be put in place to ensure that:

- Encryption facilities in use should meet international security standards or requirements;
- Staff in-charge of encryption facilities are well trained and vetted. This is verified through professional and academic testimonials, character reference from independent referees, certificates of good conduct;
- Encryption strength is adequate to protect the confidentiality of the information;
- Effective and efficient key management procedures, especially key lifecycle management and certificate lifecycle management, are in place.

5.12 Computing Equipment

5.12.1 Institutions should put in place an effective and efficient system of securing all end-user computing equipment which include desktop personal computers (PCs), portable PCs, teller terminals, automatic teller machines (ATMs), passbook printers, debit, or credit card readers, point of sale (POS) terminals, personal digital assistant (PDAs), tablet devices and smartphones, and conduct periodic security checks on all ICT equipment.

5.13 Handling Consumer Information

5.13.1 Institutions should put in place a set of policies and procedures to govern the collection, processing, storage, transmission, dissemination, and disposal of customer information.

5.13.2 In addition, institutions must ensure that they are compliant with all applicable Zambian information communication technology laws and regulations including but not limited to the Data Protection Act, 2021.

5.14 Training

5.14.1 All employees, including contract staff, should be provided with the necessary training to fully understand the institutions ICT policies, procedures, and the consequences of their violation. Institutions should adopt a zero-tolerance policy against ICT security violation.

5.15 System Acquisition, Development, Testing and Maintenance

5.15.1 System Development

- Institutions should have the capability to identify, plan, acquire, develop, test, deploy, maintain, upgrade, and retire information systems.
- Policies and procedures should be in place to govern the initiation, prioritization, approval, and control of ICT projects.
- Progress reports of major ICT projects should be submitted to and reviewed by the ICT Steering Committee periodically.
- Decisions involving significant change of schedule, change of key personnel, change of vendors, and major expenditures should be included in the progress report.

5.15.2 Project Risks

Institutions should recognize the risks associated with ICT projects, which include the possibilities of incurring various kinds of operational risk, financial losses, and opportunity costs stemming from ineffective project planning or inadequate project management controls of the CMO. Therefore, appropriate project management methodologies should be adopted and implemented to control the risks associated with ICT projects.

5.15.3 System Development Methodology

Institutions should adopt and implement a system implementation methodology to control the life cycle of Information systems. The typical phases of system life cycle include system analysis, design, development or acquisition, testing, trial run, deployment, maintenance, and retirement. The system implementation methodology to be used should be commensurate with the size, nature, and complexity of the ICT project.

5.15.4 Reliability, Integrity, and Relevance

Institutions should ensure system reliability, integrity, and relevance by controlling system changes with a set of policies and procedures, which should include the following elements:

- Ensure that production systems are separated from development or testing systems;

- Separating the duties of managing production systems and managing development or testing systems;
- Prohibiting application development and maintenance staff from accessing production systems under normal circumstances unless management approval is granted to perform emergency repair, and all emergency repair activities should be recorded and reviewed promptly;
- Progressing changes of ICT system configuration from development and testing systems to production systems should be jointly approved by the ICT function and business lines, properly documented, and reviewed periodically.

5.15.5 Data Integrity, Confidentiality, and Availability

Institutions should have in place a set of policies, standards, and procedures to ensure data integrity, confidentiality, and availability. These policies should be in accordance with the latest international data integrity and information security standards e.g., ISO 27001.

5.15.6 System upgrade

Institutions should have a set of policies and procedures controlling the process of system upgrade. The underpinning software, namely, operating system, database management system, middleware, must be upgraded, or the application software has to be upgraded. The system upgrade should be treated as a project and managed by all pertinent project management controls including user acceptance testing.

5.16 ICT Operations

5.16.1 Physical and Environmental Controls

Institutions should consider fully the environmental threats (e.g., proximity to natural disaster zones, dangerous or hazardous facilities or busy/major roads) when selecting the locations of their data centers. Physical and environmental controls should be implemented to monitor environmental conditions that could affect adversely the operation of information processing facilities. Equipment facilities should be protected from power failures and electrical supply interference.

5.16.2 Access by Third-party Personnel

In controlling access by third-party personnel (e.g., service providers) to secured areas, proper approval of access should be enforced, and their activities should be closely monitored. It is important that proper screening procedures including verification and background checks, especially for sensitive technology-related jobs, are developed for permanent and temporary technical staff and contractors.

5.16.3 Segregation of Duties

Institutions should separate ICT operations or computer center operations from system development and maintenance to ensure segregation of duties within the ICT function. The Institutions should document the roles and responsibilities of data center functions.

5.16.4 Documentation of operational instructions

Institutions should detail operational instructions such as computer operator tasks, job scheduling and execution in the ICT operations manual. The ICT operations manual should also cover the procedures and requirements for on-site and off-site backup of data and software in both the production and development environments (i.e., frequency, scope, and retention periods of back-up).

5.16.5 Problem management

Institutions should have in place a problem management and processing system to respond promptly to ICT operations incidents, to escalate reported incidents to relevant ICT management staff and to record, analyze and keep track of all these incidents until rectification of the incidents and the causes analyzed. A helpdesk function should be set up to provide front-line support to users on all technology-related problems and to direct the problems to relevant ICT functions for investigation and resolution.

5.16.6 System monitoring

Institutions should implement a process to ensure that the performance of application systems is continuously monitored, and exceptions are reported in a timely and comprehensive manner. The performance monitoring process should include forecasting capability to enable exceptions to be identified and corrected before they affect system performance.

5.16.7 Capacity plan

Institutions should develop a capacity plan to cater for business growth and transaction

increases due to changes of economic conditions. The capacity plan should be extended to cover back-up systems and related facilities in addition to the production environment.

5.16.8 Record keeping

Institutions should ensure the continued availability of technology related services with timely maintenance and appropriate system upgrades. Proper record keeping (including suspected and actual faults and preventive and corrective maintenance records) is necessary for effective facility and equipment maintenance.

5.16.9 Change management

Institutions should have an effective change management process in place to ensure integrity and reliability of the production environment. Institutions should develop a formal change management process.

5.17 Business Continuity Management

5.17.1 BCP plans

Institutions should have in place appropriate arrangements, having regard to the nature, scale, and complexity of its business, to ensure that it can continue to function and meet its regulatory obligations in the event of an unforeseen interruption in ICT. These arrangements should be regularly updated and tested to ensure their effectiveness.

5.17.2 Documentation

Institutions should document their strategy for maintaining continuity of its operations, and its plans for communicating and regularly testing the adequacy and effectiveness of this strategy.

5.18 Outsourcing

5.18.1 Supervisory Duties

Institutions should not contract out their obligations to regulatory authorities and should take reasonable care to supervise the discharge of outsourced ICT functions.

5.18.2 Critical ICT Functions

As outsourcing of data center, (ICT infrastructure, etc.), and should notify the Commission when they intend to enter into such material outsourcing arrangement.

5.18.3 Risk Analysis

Before entering into, or significantly changing, an outsourcing arrangement, the Institution should:

- Analyze how the arrangement will fit with its ICT organization and reporting structure; business strategy; overall risk profile; and ability to meet its regulatory obligations;
- Consider whether the arrangements will allow it to monitor and control its operational risk exposure relating to the outsourcing;
- Conduct appropriate due diligence of the service provider's financial stability, expertise and risk assessment of the service provider, facilities, and ability to cover the potential liabilities;
- Consider how it will ensure a smooth transition of its operations from its current arrangements to a new or changed outsourcing arrangement (including what will happen on the termination of the contract); and
- Consider any concentration risk implications such as the business continuity implications that may arise if a single service provider is used by several firms.

5.18.4 Data Security

The Institution should enhance the management of ICT-related outsourcing by putting in place measures to ensure data security of sensitive information such as customer information. Such measures include;

- Ensure that there is clear separation between outsourced information and other information handled by the service provider;
- The staff of the service provider should be authorized on "need to know" and "minimum authorization" basis;
- Ensure that service provider guarantees that its staff meet the confidential threshold required;

- Ensure all related sensitive information are deleted from the service provider's storage when terminating the outsourcing arrangement.

5.18.5 Contingency Plan

The institution should ensure that it has appropriate contingency plans in the event of a significant loss of services from the service provider. Particular issues to consider include a significant loss of resources, turnover of key staff, or financial failure of, the service provider, and unexpected termination of the outsourcing agreement.

5.19 Internal Control and Audit

5.19.1 Systems Audit

Depending on the nature, scale, and complexity of their business, it may be appropriate for institutions to combine their internal systems audit with the internal audit function. However, institutions that have capacity and the relevant competences are advised to separate systems audit from internal audit function.

1.1.2 The internal audit function should be adequately resourced and staffed by competent individuals, be independent of the day-to-day activities of the institution and have appropriate access to the institution's records.

5.19.2 Role of Internal Audit

Whether performed by a separate specialized ICT audit function or as a function within the internal audit, the responsibilities of the ICT audit function are:

- To establish, implement and maintain an audit plan to examine and evaluate the adequacy and effectiveness of the institution's systems and internal control mechanisms and arrangements;
- To issue recommendations based on the result of work carried out;
- To verify compliance with those recommendations;
- To carry out special audit on the information system. This involves investigating, analyzing, and reporting on the information system as a result of an information security incident or from a risk assessment report by the internal audit or risk management function.

5.19.3 Frequency of IT Internal Audit

Based on the nature, scale and complexity of its business, deployment of information and communication technology and ICT risk assessment, institutions should determine the scope and frequency of ICT internal audit. However, a comprehensive ICT internal audit shall be performed at a minimum once every 2 years.

5.19.4 Implementing System Development

Institutions should engage their Internal Audit and Risk Management functions when implementing system development of significant size and scale to ensure it meets the ICT Risk standards of the institution.

5.20 ICT External Audit

5.20.1 The ICT external audit should at minimum cover the following aspects:

- Risk assessment of the ICT systems.
- Review of the ICT Policies, strategy, and direction.
- Business continuity management program.
- Systems change control process.
- Reporting, logging, and auditability of the systems.
- Input-process-output controls.
- Adequacy of identification and authentication system.
- Protection against malicious malware.
- Operations and network management.

5.20.2 Institutions should ensure that the ICT external auditor reviews and examines institutions hardware, software, documentation, and data to identify all potential ICT risks.

5.20.3 Institutions should ensure that the ICT external auditors strictly comply with the law and regulations by maintaining the confidentiality of private information accessed while conducting the ICT audit. ICT audits may be carried out by external auditors or specialized firms and should be conducted at least once every two years.

SECTION 6: CREDIT RISK

6.1 Definition of Credit risk

6.1.1 Credit risk is the risk that arises from a counterparty's potential inability or unwillingness to fully Credit risk is the risk that arises from a counterparty's potential inability or unwillingness to fully meet its on and / or off-balance sheet contractual obligations. Exposure to this risk occurs any time funds are extended, committed, or invested through actual or implied contractual agreements. Credit risk cay be defined as the risk of loss arising from the failure of a counterparty to perform its obligations under a contract. Counterparties include issuers, brokers, investors, guarantors, and other capital market players who assume contractual obligations.

6.1.2 The table below shows some types and examples of credit risk:

Type of Credit Risk	Examples of credit risk
Default Risk	Failure to receive payment for transaction done on credit from a counterparty e.g., derivatives or securities
Concertation Risk	Associated with exposure of any single entity or group with the potential to produce large losses to threaten the core operations of the CMO. This may arise in form of single entity exposure or industry concentration. E.g., the US burst subprime lending crisis in 2008

6.1.3 Credit Risk exposure may be faced by the CMO itself as a result of activities that result in assets that sit on its own balance sheet. However, the credit risk may apply to clients whose assets are managed by the CMO. In line with treating customers fairly, the CMOs are expected to manage credit risk in a way that protects its client. The table below summarizes how credit risk may arise in various types of CMOs:

Type of CMO	Credit risk exposure
Clearing & Settlement Agency	Settlement risk is the possibility that one or more parties will fail to deliver on the terms of a contract at the agreed-upon time. This risk may arise if the CSA does not have a settlement guarantee scheme or insurance. Settlement Default risk is a type of settlement risk arising from the possible failure by a counterparty to deliver on a contract entirely. Settlement timing risks arise in potential situations where securities are exchanged as agreed, but not in the agreed-upon time frame. This is more critical where there are prescribed settlement times e.g., T+3 or High Frequency Trading situations. Exposure to other forms of credit risk arising from normal business transactions such as:

	• Guarantor risk: arises where the CMO acts as the guarantor of an issuer as it may incur a loss should the issuer default. On the other hand, the CMO may face credit risk due to the insolvency of the guarantor of an issuer it has invested in failing to make timely settlement. • Loans and advances to third parties and/or related parties • Issuer risk arising from investments in debt securities of other entities
Stockbrokers, Bank Dealers	• Stockbrokers and Bank dealers may be exposed to settlement Risk if pre-funding arrangements for purchase of securities are not complied with. This Pre-settlement risk is normally managed by insisting that clients pre -fund their trades before executing the orders. • May also be exposed to delivery risk in OTC transactions, as the counter party may fail to deliver according to the contract
Investment Advisers & Credit Rating Agencies	Generally, not exposed to credit risk as they do not take positions on behalf of clients. But may face exposure to credit risk arising from normal business transactions such as: • Loans and advances to third parties and/or related parties • Investments in debt securities of other entities
Fund Managers and Collective investment schemes	Generally exposed to credit risk if they do take positions on their own behalf. Also face exposure to credit risk arising from normal business transactions such as: • Loans and advances to third parties and/or related parties • Investments in debt securities of other entities The Funds under their management however face credit risk because they take positions which impact their balance sheets

6.2 Drivers of Risk

(1) Credit exposure: related to the amount of loss in the event that a counterparty defaults e.g., a trade of K500,000 is done and the counterparty defaults (does not make the payment after having promised to do so).

(2) Probability of default: the probability that the counterparty will fail to perform a contractual obligation. This will reflect the current creditworthiness of the counterparty and its prospective creditworthiness over the lifetime of any transaction. Probability of default depends on the counterparty's vulnerability to asset price movements e.g., regularly reviewing or checking credit score of the counterparty

(3) Recovery rate: the proportion of the market value of a position that is expected to be recovered if the counterparty defaults.

6.3 The key drivers of Credit Risk

- Capacity or ability to repay liabilities out of income: e.g., if the counterparty faces challenges with generating adequate income and cannot pay its obligations; review of the counterparty's financial position, quality of its financial statements and past financial performance;
- Capital or availability of financial resources available to meet commitments should income not materialize: The counterparty may not be well capitalized and hence may be unable to meet its obligations, e.g., assessing the counterparty's capital adequacy
- Impact of general economic environment on the enterprise: The counterparty may be directly affected by general economic activities that may impact its ability to meet its obligations e.g., the impact of Covid-19 on a number of companies, the competitiveness of the industry
- Target customer base: The counterparty's target customers can have an effect on the counterparty's ability generate income and/or meet its obligations e.g., targeting less credit worthy clients such as SMEs, retail clients who may include unemployed people etc.
- Lending without collateral: Lending without collateral or security provided, including the pledge of assets, guarantees from third parties, or other;
- Legal systems: Legal system that ensures enforceability of legal contracts.
- Settlement failure: Settlement failure and availability of credit default protection mechanisms e.g., settlement guarantee funds, Insurance, protection schemes, insolvency provisions.

6.4 Practical steps and guidance for the CMOs on managing the particular risk

6.4.1 Credit Risk Management

(1) Identification and assessment of the risk: it is important to have in place those that are responsible for risk management so that they are able to identify the risks through various variables such as due diligence on the counterparty. The risks should be assessed timely assess the risks.

(2) Risk Champion: a specific resource or function must be identified to be in charge of risk management so that they are responsible and accountable for it.

(3) Policies and Guidelines

(i) Policies to govern how credit risk can be mitigated through the various activities of the CMO

(ii) Procedures of how transactions should be handled with counterparties and the parameters to take into consideration beforehand

(iii) Adherence to investment guidelines prescribed in the law

(iv) Guidelines to ensure collateral based lending (transactions)

(4) Due diligence: conduct comprehensive and ongoing due diligence of counterparties as well as assessing their performance from time to time.

(5) Employ risk management safety measures such as Insurance, Settlement guarantee fund

6.5 Policies, Procedures and Limits

6.5.1 Policies relating to limits

Establishment of sound and well-defined policies, procedures and limits is vital in the management of credit risk. These should be well documented, duly approved by the board and strictly implemented by management. Credit policies establish the framework for lending and guide the credit-granting activities of the institution

An effective credit policy should outline the following:

(i) **Defines the credit concentrations, limits, and exposures** the organization is willing to assume. These limits will ensure that credit activities are adequately diversified. The policy on large exposures should be well documented to enable CMOs to take adequate measures to ensure concentration risk is mitigated. The policy will clearly stipulate the percentage of the CMO's capital and reserves that the institution can grant as loans or extend as other credit facilities to any individual entity or related group of entities.

(ii) **In the exposure limit, contingent liabilities** should be included – for example guarantees, acceptances and letters of credit. In the case of large exposures, CMOs must pay attention to the completeness and adequacy of information about the counterparty.

(iii) **Board approval:** The policy should require that the board approve all loans to related or connected parties. These credits should be based on market terms and should not be more favorable with regard to amount, maturity, rate, and collateral than those provided to other customers.

(iv) On exposure limits the policies should include the following:
- Acceptable exposure to individual counterparties
- Maximum exposure to connected groups and insider dealings.
- The total overall limit on the credit portfolio in relation to capital, assets, or liabilities.
- Limits in relation to geographical location or other segmental analysis
- Maximum exposure to individual economic sectors (for example commercial, consumer, real estate, agricultural).
- Acceptable limits on specific products.

(v) **Compliance with regulations and other policy documents:** CMOs should ensure that their own internal exposure limits comply with any regulatory requirements or other documents such as Investment Policies, Trust deeds and constitutive documents in terms of the CIS Rules.

(vi) **Communication within the organization:** In order to be effective, credit policies must be communicated throughout the organization, implemented through appropriate procedures, and periodically revised to take into account changing internal and external circumstances.

6.5.2 Segregation of Duties

Credit policy formulation, credit limit setting, monitoring of credit exposures and review and monitoring of documentation are functions that should be performed independent of the loan

origination function. For small CMOs, where it might not be feasible to establish such structural hierarchy, there should be adequate compensating measures to maintain credit discipline, introduce adequate checks and balances and standards to address potential conflicts of interest.

6.5.3 Policies relating to credit assessment and granting process

CMOs must operate under sound, well-defined credit-granting criteria. These criteria should include a thorough understanding of the borrower or counterparty, as well as the purpose and structure of the credit, and its source of repayment.

CMOs must receive sufficient information to enable a comprehensive assessment of the true risk profile of the borrower or counterparty. At a minimum, the factors to be considered and documented in approving credits must include:

- the purpose of the credit and source of repayment;
- the integrity and reputation of the borrower or counterparty;
- the current risk profile (including the nature and aggregate amounts of risks) of the borrower or counterparty and its sensitivity to economic and market developments;
- the borrower's or counterparty's repayment history and current capacity to repay, based on historical financial trends and cash flow projections;
- The borrower credit rating/report from licensed Credit Reference Bureau;
- a forward-looking analysis of the capacity to repay based on various scenarios;
- the legal capacity of the borrower or counterparty to assume the liability;
- where applicable, the adequacy and enforceability of collateral or guarantees, including under various scenarios.

6.5.4 Internal Risk Rating Systems

An important tool in monitoring the quality of individual credits, as well as the total portfolio, is the use of an internal risk rating system. A well-structured internal risk rating system is a good means of differentiating the degree of credit risk in the different credit exposures of a CMO institution. This will allow more accurate determination of the overall characteristics of the credit portfolio, concentrations, problem credits and the adequacy of loan loss reserves. In determining loan loss reserves, CMOs should ensure that the Central CMO of Kenya classification criteria are the minimum.

Typically, an internal risk rating system categorizes credits into various classes designed to take into account the gradations in risk. Simpler systems might be based on several categories ranging from satisfactory to unsatisfactory; however, more meaningful systems will have numerous ratings for credits considered satisfactory in order to truly differentiate the relative credit risk they pose.

While developing their systems, CMOs must decide whether to rate the riskiness of the borrower or counterparty, the risks associated with a specific transaction, or both. Internal risk ratings are an important tool in monitoring and controlling credit risk. In order to facilitate early identification, institution's internal risk rating system should be responsive to indicators of

potential or actual deterioration in credit risk e.g., financial position and business condition of the borrower, conduct of the borrower's accounts, adherence to loan covenants and value of collateral.

Credits with deteriorating ratings should be subject to additional oversight and monitoring, for example, through more frequent visits from credit officers and inclusion on a watch list that is regularly reviewed by senior management. The internal risk ratings can be used by line management in different departments to track the current characteristics of the credit portfolio and help determine necessary changes to the credit strategy. Consequently, it is important that the board of directors and senior management also receive periodic reports on the condition of the credit portfolios based on such ratings.

The ratings assigned to individual borrowers or counterparties at the time the credit is granted must be reviewed on a periodic basis and individual credits should be assigned a new rating when conditions either improve or deteriorate. Because of the importance of ensuring that internal ratings are consistent and accurately reflect the quality of individual credits, responsibility for setting or confirming such ratings should rest with a credit review function independent of that which originated the credit concerned. It is also important that the consistency and accuracy of ratings is examined periodically by a function such as an independent credit review group.

6.5.5 Policies on Inter-CMO transactions

Inter-CMO transactions also portend significant credit risk. These transactions are essentially for facilitation of fund transfers, settlement of securities transactions or because certain services are more economically performed by other CMOs due to their size or geographical location. An institution's lending policy should typically focus on the following:

- The establishment and observation of counter party credit limits.
- Any inter-CMO transaction for which specific provisions should be made.
- The method and accuracy of reconciliation of the nostro and vostro accounts.
- Any inter-CMO credit with terms of pricing that is not a market norm.
- The concentration of inter–CMO exposure with a detailed listing of CMOs and amounts outstanding as well as lending limits.

6.5.6 Role of Oversight Functions in managing the Risk

The Risk Management Function must ensure that potential credit risk is adequately identified, assessed, and mitigated. In addition, the risk management function must ensure that adequate controls are put in place to minimize credit risk. It should also ensure to comply with standards specified in the law, legislation, and regulation in risk management

The Compliance Function must ensure that the CMO's is in compliance with the law and their internal policies and procedures put in place to mitigate credit risk.

The Internal Audit function must ensure that they assess the effectiveness of systems and procedures that have been put in place to mitigate credit risk and recommend ways in which these can be improved in the event that weaknesses have been identified.

6.5.7 Role of Senior Management (SM)

The CMO's senior management are expected to ensure that adequate measures, including policies are put in place to help identify and minimize credit risk.

6.5.8 Role of Board of Directors

The CMO's Board of Directors must, primarily through its Risk and Audit Committee, monitor the efficiency of the Company´s internal control, internal audit (if applicable), and risk management systems. In order to do this, the Board must guarantee it is receiving adequate information regarding all these areas and that it makes sure any identified weaknesses are addressed appropriately and in a timely manner.

6.6 Role of Oversight Functions in managing the Credit Risk

6.6.1 The Risk Management Function must ensure that potential credit risk is adequately identified, assessed, and mitigated. In addition, the risk management function must ensure that adequate controls are put in place to minimize credit risk. It should also ensure to comply with standards specified in the law, legislation, and regulation in risk management

6.6.2 The Compliance Function must ensure that the CMO's is in compliance with the law and their internal policies and procedures put in place to mitigate credit risk.

6.6.3 The Internal Audit function must ensure that they assess the effectiveness of systems and procedures that have been put in place to mitigate credit risk and recommend ways in which these can be improved in the event that weaknesses have been identified.

SECTION 7: MARKET RISK

7.1 Definition of Market Risk

7.1.1 Market risk is the risk arising from movements of interest rate, foreign exchange rate, and prices of instruments in the capital and money markets which negatively affect the earning and capital of the CMO. Market risk can be classified into the following:

(1) **Interest Risk:** the risk that earnings or capital of the CMO may be affected from changes in interest rates of assets, and debts.
Interest risk arises from the CMOs balance sheet exposure to interest bearing assets and liabilities. These include customer deposits, loans, bonds and financial derivates products.

(2) **Currency Risk**: the risk that earnings or capital may be affected from fluctuations of exchange rate, due to a transaction in a foreign currency or from holding an asset, liability, or debt in a foreign currency.

Examples of items that contain currency risk include, assets and liabilities denominated in foreign currency, foreign exchange transactions, derivates of foreign exchange transactions (forwards contracts, futures, swaps, options, etc., assets and liabilities whose cash flow (redemption value, coupon rate, etc. is determined in reference to foreign exchange rates.

(3) **Price risk** the risk that earnings or capital may be negatively affected from changes in the price of debt or equity instruments. This causes the value of the investment in the trading portfolio and profit to diminish.

Examples of items that contain price risk include stock prices, corporate bonds with equity purchase warrants, stock derivates (forward contracts, futures. swaps, option, etc.).

(4) **Commodity Risk:** the likelihood that a commodity price, such as that of a metal or grain, will change.

Examples of items that contain commodity risk include, commodity derivates (forwards, futures, swaps, options, etc.) and assets and liabilities whose cash flow (redemption value, coupon rate, etc.) is determined in reference to commodity prices, commodity index prices, etc.

(5) **Inflation Risk:** the risk that overall rises in prices of goods and services will undermine the value of money, and probably adversely impact the value of investments.

7.1.2 In managing market risk, CMO s need to have five fundamental management factors as follows

- Risk Management Policy

- Board of Directors
- Senior Management
- Risk Champion
- Internal Control and Audit

7.1.3 It is important to review whether the market risk management system developed is an appropriate one suited to the CMO's strategic objectives, the scale and nature of its business and its risk profile.

7.2 Market Risk Management

7.2.1 Risk Management policy

7.2.1.1 The CMO should have a risk management policy that guides the CMO on market risk. The risk management policy should covert the appropriateness of the market risk in the risk management policy which should among others include clear statements such as

- the roles and responsibilities of the board of directors and senior management with regards to market risk.
- clearly defined market risk limits
- clear lines of authority and responsibilities for managing market risk exposure.
- Identification, assessment, monitoring, control, and mitigation of market risk.
- Whether the CMO does revise its market risk policy in a timely manner by reviewing its effectiveness based on reports and findings on the status of market risk management in regular and timely manner or on an as needed basis.

7.3 Board of Directors

7.3.1 The CMO should ensure there is Board oversight. The CMO's board of directors should understand the character and existing levels of risks that befit the CMO's business strategies and mechanisms for risk management. Effective risk management should have reporting to the board through the Risk and Audit Committee on the market risk management on a regular basis and timely for the board to make an appropriate assessment and judgement about the status of the market risk management and the status of market risks.

7.3.2 The reporting of market risk should among other include:

- The market risk profile and trends;
- The status of compliance with risk limits and the status of the application; and
- The nature (limitations and weaknesses) and validity of the market risk measurement and analysis method.

7.3.3 The board of directors of the CMO should consist of people with diverse experiences, possessing an understanding of the business of the CMO and market risk management. The board of the CMO will have the following responsibilities

- to establish strategies and risk tolerance levels;

- to appoint senior management with authority to be responsible for risk management;
- to monitor performance and overall market risk of the CMO to ensure that it is managed
- to ensure that the CMO develops basic guidelines in specifying, measuring, monitoring, and reporting market risks.
- to arrange to have suitable and sufficient staff with capability in market risk management.

7.4 Senior Management

7.4.1 The senior management of the CMO has the responsibility of implementing all approved policies that govern Market Risk and developing procedures for effective management of the risks.

7.4.2 Management should be mandated by the board to be responsible for maintaining:

- appropriate limits on risk taking; the risk limit should be in line with the measurement method and depends on the level of capital, performance, and risk tolerance of the CMO. The risk limit should match the size, the complexity of the business of the CMO and the adequacy of the CMO's capital
- adequate systems and standards for measuring market risk;
- standards for valuing positions and measuring performance;
- a comprehensive market risk reporting and review process.
- effective internal controls.

7.4.3 Management should be sufficiently competent and able to respond to price risks, interest risks and foreign exchange risks that may arise from changes in the competitive environment or from innovations in markets in which the institution is active.

7.5 Risk Champion and staff

7.5.1 The CMO should a senior member of staff to head the risk management function with the necessary knowledge and experience. The risk management function should have adequate number of staff to with the necessary knowledge and experience to execute the relevant operations and assigned such staff the authority necessary for implementing the operations.

7.6 Internal Controls and Audit

7.6.1 The CMO should have adequate internal controls to ensure the integrity of their market risk management process. These internal controls should be an integral part of the CMO's overall system of internal control. The CMO should be audited by internal audit to assess the effectiveness of the market risk controls in place and to appropriately identify matters to be audited with regards to market risk management. The internal audit report on market risk should among indicate They should promote

- status of compliance with market risk policy or guidelines;
- appropriateness of the market risk management processes commensurate with the scale

and nature of the business and risk profile;

- appropriateness of the use of market risk measurement and analysis methods (techniques, assumptions, etc.) taken into account;
- validity of the market risk measurement and analysis methods
- accuracy and completeness of the data used in market risk measurement and analysis
- status of improvement of matters pointed out in an internal audit or on the occasion of the late inspection.

7.6.2 The internal audit function of the financial institution should review and assess the market risk management process and ensure that management observe the laid down policies and procedures governing market risk management and that accounting procedures meet the necessary standards of accuracy, promptness, and completeness.

SECTION 8: Legal and Regulatory Risk

8.1 Definition of Legal and Regulatory Risk

8.1.1 Regulatory compliance risk arises from a CMO's potential non-conformance with laws, rules, regulations, prescribed practices, or ethical standards in any jurisdiction in which it operates.

8.1.2 The table below provides examples of legal and regulatory risks that could arise categorized in line with the above definition:

Source of risk	Examples of legal and regulatory risks
Internal Risk	• No legal department. • Inadequate legal team experience and skill set sufficient to identify and address organization's objectives and risk level. • Lack of independence in recruiting process and undefined recruitment criteria. • Lack of capacity building or training programs to ensure compliance with emerging industry and regulatory practices • Lack of understanding of key functions of legal department. • No systems for tracking legal matters • Inadequate and/or lack of continuing monitoring process of legal department deliverables. • Inadequate or insufficient documentation and record keeping.
External Counsel	• No clear policy for retaining external counsel and no framework to determine which work is to be handled internally and which work requires external counsel. • Failure to undertake or no internal policy for conflict checks before engaging external counsel. • Excessive legal costs. • Failure to provide specific contact person for reporting and issuing instructions to external counsel. • No policy for minimum requirements external counsel must have before retainer. E.g., valid professional insurance cover. • No systems for tracking progress and reports for instructions given to external counsel
Legal framework and change of law	• Increased cost of operation caused by new regulatory obligation. • Ambiguous legislation. • Lack of law review policy. • Lack of understanding of regulatory framework and impact on business prior to, and after enactment.

	• Lack of system to ensure period gap analysis reviews relating to regulatory framework and internal policies and/or corporate governing documentation.
Litigation Risk	• Frivolous actions • Failure to ascertain prospects of success on an action and making provision in case of unfavorable judgments. • Failure to employ alternative dispute resolutions • Failure to recognize litigious matter and seek ex-curia settlement • Cost escalation through prolonged litigation
Contract and transactional risks	• Lack of legal involvement in contract formation process including negotiations for complex transactions. • Inadequate drafting skills. • Invalid form of contract. • Lack of appreciation of risk associated with transaction. • Inadequate information on contracting parties and ability to perform arising contractual obligations. • Poorly drafted contract terms with ambiguous clauses on rights, obligation and benefits accruing. • Inadequate or poorly drafted risk mitigating measures in contracts. • Inadequate control measures for execution of contracts. • Lack of or inadequate clauses spelling out pre-contractual obligations. • Lack of enforcement clauses in case of breach of obligation. • Failure to complete perfection or registration of interests acquired in securities and/or other assets and benefits under contracts, as required by statute e.g., registration of lease within time required by law, including equitable interests.

8.2 Drivers of Risk

1) Emerging regulations and best practices: A legal team is best suited to identify and assess legal and regulatory risk. This is a function performed by individuals and therefore, it is pertinent that an organization not only has competent persons but further makes deliberate policies and measures to ensure that such persons are adequately trained on emerging industry and regulatory best practices. This includes putting measures to vet employees and any legal services to be outsourced.

2) Departmental Integration: A well functional legal team cannot operate independent of the organization, and neither can an organization perform its departmental functions without prior input of the legal team if risk is to be identified and avoided and/or mitigated.

3) Nature of Business or investment: Contracts ought to be drafted in line with risk inherent in the various areas an investment is to be made and the core business of an organization. Whilst contract precedents and forms may provide a useful refence point, understanding the law surrounding the nature of business and legal impediments in that respect, is vital to ensuring that contractual terms are not rendered impossible to perform by law.

4) Diminutive control and supervision over external service provider: An organization may have a structure where they have a small legal team and outsource most of its work to external counsel. However, it is not uncommon for organizations with huge legal teams to also outsource legal services. An organization needs to consider the risk posed by engaging external legal counsel, such as inaction on a court matter leading to court judgment and subsequent execution on an organization's assets.

5) Government policy and political regime: e.g., change in tax law policy.

6) Judicial Precedent and stare decisis: Despite incorporating adequate measures to mitigate business risk, a superior court such as the Supreme Court of Zambia may interpret new legislation (including cases to which an entity may not be a party, but materially affects such entity's business operations and practices) contrary to the way an entity interprets and applies such new law. In such a case, all lower courts and tribunals are bound to follow the decision of the high court.

7) Customer dissatisfaction: Mere customer dissatisfaction may lead to frivolous cases that may result in costly litigation and reputational damage to a business. It is therefore important to ensure that contracts are carefully drafted to exonerate an entity from liability.

8) Other external events: Despite these being outside the control of an entity, their effects could still negatively impact its business operations. It is therefore expected that entities put in place contingency plans that can be deployed in the instance of such events.

8.3 Practical steps and guidance for the CMOs on managing the particular risk

8.3.1 An entity needs to set in place policies, manuals and coded procedures and controls relating to the following (must be in line with best practices and the law):

8.3.2 Internal Risk:

- Requitement process.
- Staff Training.
- Code of Ethics and Code of conduct.
- Integrated departmental functions and procedures.
- Case management systems.
- Risk profile and scoring system.

8.3.3 External Counsel:

- External service manual with conflict check forms and procedures, matter allocation policy, minimum service charge and law firm recruitment process.
- Robust follow up processes for monthly status updates.
- Policy on CMO involvement prior to action being taken.

8.3.4 Legal framework, change of law and litigation risk:

- Robust and periodic legal review process and gap analysis of CMO policies, documentation, and level of regulatory compliance.
- Policy on stakeholder engagement on applicability of relevant legislation.
  Integrated departmental functions and procedures for decision making and legal opinions for complex decisions to be made.
- Have a system for planning and tracking statutory obligations when they become due and assign staff to attend to them to mitigate the potential risk of neglect and/or failure to comply within the stipulated timeframe specified by the law. For example, have a compliance standard procedure document with specific dates and responsible personnel.

8.3.5 External Events:

The CMO must ensure that a robust business continuity plan must be in place. This must include disaster recovery plan and provision for adverse judgments.

8.4 Role of Oversight Functions in managing Legal and Regulatory Risk

8.4.1 The Risk Management Function, Compliance Function and Internal Audit function must ensure that the CMO has:

- A designated resource responsible for each function with adequate training and sufficient experience.
- A policy for trainings of the compliance.
- A risk profile and scoring system focusing on risk inherent to nature of business undertaken.
- A legal risk policy developed in line with the CMO's risk profile, to focus on a proactive and strategic legal risk management and mitigation measures. The policy must focus on measuring risk, monitoring and management of such risk and the reporting mechanism for action (including in cases where urgent action is required).
- A risk management policy that includes accountability action that also assess effectiveness of control measures and implementation of further controls and mitigation measures.
- A compliance manual speaking to the CMO's function to ascertain the compliance philosophy of the entity and how the company intends to meet its securities business regulatory obligations.
- Compliance reviews and/or assessments conducted by the CMO and with structured reporting systems and procedures.
- System for ascertaining the compliance history of the CMO with the securities legal and regulatory framework in the recent past (e.g., circulars and guidelines).

- A framework to document new or amended existing compliance policies and communicate them across the institution on a timely basis.
- A system to promptly develop or amend the institution's compliance policies as legislation is introduced or amended or as new or changing business activities impose different legislative requirements on the institution.
- Policies and systems to assess the extent to which practices of a CMO ensure that the institution is kept abreast of new and changing legislations and changes in the institution's risk profile.

8.5 Role of Senior Management (SM)

8.5.1 The CMO's senior management are expected to ensure that adequate measures, including policies and procedures are put in place to help minimize risks. Senior management must also ensure that adequate controls are in place to ensure that policies and procedures are not only being implemented, but that they are also being implemented correctly.

8.6 Role of Board of Directors

8.6.1 The CMO's Board of Directors must, primarily through its Risk and Audit Committee, monitor the efficiency of the Company´s internal control, internal audit (if applicable), and risk management systems. To do this, the Board must guarantee it is receiving adequate information regarding all these areas and that it makes sure any identified weaknesses are addressed appropriately and in a timely manner.

SECTION 9: STRATEGIC RISK

9.1 definition of Strategic Risk

9.1.1 Strategic risk arises from a CMO's potential inability to implement appropriate business plans and strategies, make decisions, allocate resources, or adapt to changes in its business environment. The CMOs are expected to have strategic risk management processes to identify, quantify and mitigating any risk that affects or is inherent in a company's business strategy, strategic objectives, and strategy execution. At a minimum, the CMO should ensure that it has a well-documented strategic plan that is approved by its Board of Directors.

9.1.2 Importance of strategic planning

Strategic planning is necessary to determine the direction for your organization. It focuses your efforts and ensures that everyone in the business is working towards a common goal. It also helps you:

- Mission – this sets out the CMOs long term business' purpose
- Vision – sets out what the CMOs intend to achieve
- Strategic Plan – This outline how the company will achieve its Mission and Vision.

9.1.3 Strategic planning forms the basis for directing the business activities it its bid to achieve its objectives. It enables the CMO to:

- Determine/ agree activities that will contribute to business growth
- Allocate its resources for optimal results
- Determine the CMOs funding model
- Build competitive advantage
- Determine its Risk Appetite i.e., how much is the CMO willing to take in pursuit of its strategic objectives.
- Ensure adequate information and communication to CMO staff, management, and Board on what needs to be done and their respective roles and responsibilities.

9.2 Key risks/ drivers of strategic risk include:

- Shifts in consumer demand and preferences;
- Legal and regulatory changes;
- Competitive pressure – new entrants, copy-cat tactics, counterfeit products;
- Mergers/ Demergers/ integration;
- Technological changes;
- Stakeholder pressure, shareholder revolts.

9.3 Elements of the strategic management process

9.3.1 The table below illustrates the four elements of the strategic planning process. The CMO should have an understanding of its operations, activities, and its external environment in order to address each element in the process.

(1) **Where are you now?** – The starting point is to establish the status of the CMO. The CMO staff need to acquire as much Knowledge of the CMO's Business, how it operates internally, how does it generate its income, what drives its profitability, and how it compares with competitors. This can also be an opportunity for introspection and critical review of the CMOs business. This process should also consider the above risk drivers.

(2) **Where do the shareholders/ Board and/or Senior Management want to take the CMO?** – Desired Strategic outcomes specificizing between Long, Medium Term and Long Term? What are the key focus areas etc.

(3) **How will the CMO you get to its desired position?** - Map out the journey, the milestones, and the changes you will need to make to meet your strategic objectives.

(4) **How will the CMO ascertain that it is succeeding?** – Definition of success, review checkpoints and measurement of success.

9.4 The Strategic Planning Process: policies and procedures

9.4.1 A typical strategic planning process follows the steps outlined below:

9.4.2 The Board or more accurately, Senior Management will determine how the above steps are undertaken. The commonest approaches include:

(i) Delegating to a dedicated strategy team, who then arrange a series of meetings (including some with key staff) and delegating sections to team members to draft. The strategy could hold brain storming session, meetings with stakeholder or survey key stakeholders to gain information required to address the elements of strategic planning above.

(ii) Outsourcing the exercise to an outside professional to undertake the process on behalf of management.

9.5 The Strategic Planning Process: policies and procedures

9.5.1 Effective management of strategic risk requires that a CMO establishes policies, procedures, and limits to ensure objective evaluation of and responsiveness to a CMO's business environment.

9.5.2 CMOs should have a documented and Board approved process for formulating and approving the strategic plan. This process and all related procedures, including the responsibilities of the Board and senior management and other staff concerned, should be clearly documented, approved by the Board, and subject to periodic review to ensure their appropriateness.

9.5.3 Policies on business strategy should address the following:

(i) A definition of the critical business segments/ processes/ activities/ products that the CMO will focus in the short, medium, and long term

(ii) Definition of the frequency and procedure for review of the CMO's business strategy.

(iii) A requirement that the CMO should operate based on a Board approved strategic plan;

(iv) Transitional provisions where a CMO's strategic plan is not concluded in time following expiry of a previous plan.

9.5.4 Procedures for defining and reviewing the institutions' business strategy are intended to ensure that the following aspects are given adequate consideration:

- The CMO's inherent strengths.
- Its identified weaknesses.
- Opportunities external to the institution.
- External factors that pose threats to the institution.

9.5.4.1 The following tools can be used to identify the above

- SWOT Analysis
- PESTEL Analysis
- Porters 5 Forces

9.5.5 Limits are necessary in defining the CMOs risk appetite including:

- Exposure to different sectors.
- Growth of business and staff strength.

9.6 Procedures for developing a strategic planning

9.6.1 This section provides guidance on specific steps a CMO can follow to develop and implement a strategic plan. These are summarized in the table below:

#	Stage in strategic planning process	Expected procedures/ outcomes	Tools that can be used
1	**Analysis & goal setting Analysis**	Situational analysis which in turn helps the CMO: • Define **Vision** • Define **Mission** • Define its Strategic **Objectives** • Define strategic **Goals** • Define its **Values**	• SWOT Analysis • PESTEL Analysis • Porters 5 Forces • Gap Analysis • Balanced Score Cards

			• Guidance from the Shareholders/ Board/ Senior Management and other stakeholders' direction on aspirations
2	**Strategy formulation**	• **Strategic Plan** – Long term plan • **Business Plan** – normally short term and addressing a particular aspect of the long-term strategy • **Contingency Plan** – to address an emergency that threatens the existence of the CMO.	Based on the analysis of the Opportunities and threats identified from the analysis stage and the optimization and mitigation measures identified by the CMOs strategy team.
3	**Implementation of strategy**	Change management processes	Implementation Plan Performance Management Tools – e.g., BSC
4	**Monitoring and evaluation**	PMS Periodic Reviews (at least once annually by BoD, Quarterly for SM and more frequently for other operational management and staff	Performance Management Systems targeting the CMO as a whole and cascaded to individual members of staff in the organization.

9.7 Goal setting and analysis

9.7.1 In setting strategic goals and objectives, the CMO should be guided by their corporate mission which outlines the direction the CMO is expected to follow, and which reflect the vision and values it upholds.

9.7.2 Strategic goals should reflect the CMOs aspirations in achieving a specific target e.g., Growth and return, efficiency gains, competitive advantage within the environment it operates.

9.7.3 In setting strategic goals and objectives, institutions identify and consider the needs and aspirations of their major stakeholders and changes in operating environment as identified using the analytical tools highlighted above.

9.7.3.1 The Balanced Score Card is a tool that CMOs can utilities to document how the proposed strategy will enable them to achieve the desired objectives.

Source: BSC Institute

9.8 Strategy formulation

9.8.1 **Assessment of the results of strategic analysis:** CMOs should have a process for evaluating their strategic position and developing appropriate strategies to achieve their strategic position and developing appropriate strategies to achieve their strategic goals and objectives. This should be based on the CMOs understanding of the CMOs general business and economic environment and identification of strength and weaknesses and establish its strategic position.

9.8.2 **Identification of possible strategies:** based on the analysis the CMO should identify and assess possible optimization strategies (to take advantage of strengths and opportunities) and mitigation strategies (to address the weaknesses and threats) that can be considered having regards to its stated goals and objectives and risk tolerance.

9.8.3 **Formulation and documentation of strategic plan:** Strategic decisions agreed upon during the planning process should form the basis of the strategic plan. Apart from describing what strategies the institution will take and how the institution will implement them to meet its strategic goals and objectives, the plan should also provide other information, such as the institution's philosophy towards its business, its growth targets, the extent of its financial risk-taking, and other relevant factors (institutional and environmental) affecting its growth and development. The depth and coverage of the strategic plan should be commensurate with the institution's scale and complexity of business.

Contents of a Strategic Plan

- **Executive summary:** This can be useful for prospective investors and other key external stakeholders.
- **Core values -** outlining the principles that underpin your business culture.
- **Mission statement -** describing the long-term purpose of your business.
- **Problem statement -** explaining key issues that you wish to address.
- **SWOT/ PESTEL analysis -** examining your business' internal strengths and weaknesses, as well as external opportunities and threats. See a SWOT analysis example.
- **Objectives and goals -** outlining your top-level objectives as measurable and actionable steps. These might include attracting a new type of customer, developing new products and services, or securing new sources of finance.
- **Implementation plan -** setting out key actions (with desired outcomes and deadlines) needed to fulfil your top-level objectives.
- **Monitoring and evaluation -** determining which key performance indicators (KPIs) you will track, and how you will monitor the progress against actions on an ongoing basis.
- **Resourcing -** summarizing the impact of the proposed strategy on resources, including budget, staffing, premises, and equipment.

Source: https://www.nibusinessinfo.co.uk/content/how-do-you-develop-strategic-plan

9.9 Strategy implementation

9.9.1 Alignment and change management

Before implementing its strategy, the CMO should ensure that there is alignment of internal resources and processes including change management issues such as:

- Mindset/ Culture changes – It is important for the Board and Senior Management to set the tone at the top by showing support for the strategic planning process and the strategy adopted by the CMO.
- Organizational restructuring required to facilitate the achievement of desired outcomes.
- Business Process re-engineering to address follow of information and transactions/ Interdependencies between processes/ department.

9.9.2 Alignment of internal resources and processes means includes ensuring the following:

- sufficient resources (financial and non-financial) have been allocated to undertake the necessary tasks;
- the CMO has the right mix of skills and numbers allocated for the performance of various tasks in the strategy implementation including for the monitoring and evaluation; and
- the organization and risk management structure, systems, infrastructure, and technology are in the right shape to support the new initiatives.

9.9.3 Planning and Management of Capital and Funding needs

9.9.3.1 Inadequate planning of capital and funding needs is an obstacle to implementing strategic decisions and can have a disruptive effect on an institution operation and its ability to meet

strategic goals and objectives. Institutions should view planning for capital and funding should be included as part of the strategic planning process.

9.9.3.2 Capital planning should be risk-based and forward-looking and consider such factors as an institution's current and future capital needs, anticipated capital expenditures, dividend payment forecasts, desirable capital levels, and external capital sources (e.g., available supply of capital and capital raising options).

9.9.3.3 CMOs should at a minimum produce the following forecasts:

- Forecast Profit and loss (Income and expenditure)

FORECAST PROFIT AND LOSS - PROFORMA	YEAR 1 ZMW	YEAR 2 ZMW	YEAR 3 ZMW	YEAR 4 ZMW	YEAR 5 ZMW
Revenues	100,000	150,000	300,000	750,000	2,250,000
Cost of services provided	(25,000)	(38,000)	(75,000)	(188,000)	(563,000)
Gross profit	**75,000**	**112,000**	**225,000**	**562,000**	**1,687,000**
Other operating income	35,000	53,000	106,000	159,000	477,000
Other operating expenses	(9,000)	(13,000)	(27,000)	(40,000)	(119,000)
EBITDA	**101,000**	**152,000**	**304,000**	**681,000**	**2,045,000**
D&A	(30,000)	(60,000)	(90,000)	(120,000)	(150,000)
Operating income	**71,000**	**92,000**	**214,000**	**561,000**	**1,895,000**
Financial income	191,000	197,000	95,000	104,000	189,000
Finance expenses	(60,000)	(72,000)	(74,000)	(75,000)	(75,000)
Profit before tax	**202,000**	**217,000**	**235,000**	**590,000**	**2,009,000**
Corporation tax	(71,000)	(76,000)	(82,000)	(207,000)	(703,000)
Profit after tax	**131,000**	**141,000**	**153,000**	**383,000**	**1,306,000**

- Forecast statements of financial position (Balance sheets)

FORECAST STATEMENT OF FINANCIAL POSITION (BALANCE SHEET) - PROFORMA					
ASSETS	YEAR 1 ZMW	YEAR 2 ZMW	YEAR 3 ZMW	YEAR 4 ZMW	YEAR 5 ZMW
Property and equipment	120,000	210,000	270,000	300,000	300,000
Government Securities - Bonds	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000
Investments in listed equities	296,000	343,000	288,000	242,000	281,000
Amounts due from related parties	162,000	276,000	359,000	422,000	473,000
Trade and other recievables	135,000	238,000	394,000	753,000	2,180,000
Cash on hand and balances with banks	107,000	32,000	80,000	214,000	566,000
TOTAL ASSETS	**1,820,000**	**2,099,000**	**2,391,000**	**2,931,000**	**4,800,000**
LIABILITIES & EQUITY					
LIABILITIES					
Loans and borrowings	360,000	372,000	374,000	375,000	375,000
Trade and other payables	89,000	139,000	201,000	344,000	808,000
Income tax	7,000	8,000	8,000	21,000	70,000
Amounts due to related parties	425,000	425,000	425,000	350,000	325,000
	881,000	**944,000**	**1,008,000**	**1,090,000**	**1,578,000**
CAPITAL AND RESERVES					
Share Capital	150,000	200,000	250,000	300,000	350,000
Share Premium	350,000	375,000	400,000	425,000	450,000
Retained Earnings	439,000	580,000	733,000	1,116,000	2,422,000
	939,000	**1,155,000**	**1,383,000**	**1,841,000**	**3,222,000**
TOTAL CAPITAL AND RESERVES	**1,820,000**	**2,099,000**	**2,391,000**	**2,931,000**	**4,800,000**

- Forecast Cashflows

The table below illustrates a proforma cashflow forecast which indicates the CMO expects to have sufficient resources to fund its operations

FORECAST CASHFLOWS- PROFORMA					
	YEAR 1 ZMW	YEAR 2 ZMW	YEAR 3 ZMW	YEAR 4 ZMW	YEAR 5 ZMW
Opening balance	758,000	107,000	32,000	80,000	214,000
Capital injection	50,000	75,000	75,000	75,000	75,000
Receipts from debtors	-	100,000	250,000	550,000	1,300,000
Loans disburseed	300,000	-	-	-	-
Advances from related parties	500,000	100,000	75,000	25,000	100,000
Coupons received	150,000	150,000	150,000	150,000	150,000
Receipts from related parties	88,000	149,000	193,000	227,000	254,000
Bond purchases	(1,000,000)	-	-	-	-
Purchase of listed securities	(255,000)	-	-	-	-
Advances to Related Parties	(250,000)	(263,000)	(276,000)	(290,000)	(305,000)
Loan repayments	-	(60,000)	(72,000)	(74,000)	(75,000)
Payments Creditors	(95,000)	(151,000)	(190,000)	(235,000)	(368,000)
Taxes paid	(64,000)	(75,000)	(82,000)	(194,000)	(654,000)
Payments to related parties	(75,000)	(100,000)	(75,000)	(100,000)	(125,000)
	107,000	**32,000**	**80,000**	**214,000**	**566,000**

9.9.3.4 The above forecasts are based on the information obtained from the strategic planning process and may include some of the following building block numbers that financial forecasts need:

- Revenue Targets
- Quarterly gross margin targets
- Expense to revenue ratios for major expense categories like sales, general and administrative, and indirect labor
- Major fixed expenses like rent or debt servicing
- Quarterly net profit targets
- Accounts Receivables and Accounts Payables average terms
- Planned Capital expenditure
- Planned Borrowings to finance Capex and Opex
- Planned Investment activities
- Targeted economic capital vs statutory regulatory capital requirements

The above should reflect the way the CMO anticipates implementing its strategy. The information should be analyzed for the entire strategic period and broken down into Annual, Quarterly, or monthly revenue targets for forecasting purposes.

9.9.4 Information and communications systems

The ability to effectively manage information is crucial to an institution's ability to implement its strategic objectives and respond to changes in its operating environment. This will enable the CMO will remain competitive, introduce new products and services, and achieve desired goals. Institutions should therefore ensure that they have sufficient and robust MIS to support their strategic planning and decision-making processes.

9.9.5 Human resources management and development

Human resources management has a strategic focus in that it is involved in gaining commitments to an institution's goals and shaping its corporate culture. By developing policies to meet future needs, human resources management enables the adoption of a forward-looking approach to deal with change and growth and to anticipate future problems.

9.9.6 Succession Planning

The institutions' management should develop management succession plans to cater for staff turnover and retirement. This is particularly essential for institutions to cater for major turnover in senior and middle management, whether due to transfer, resignation, or retirement.

9.9.6.1 The institutions' board of directors should also maintain succession plans for critical positions such as Chairman of the Board and the institution's Chief Executive Officer.

9.9.7 Stress-Testing and Contingency Strategies

Institutions should employ stress-testing techniques in their strategic planning and management processes to assess any potential threats to the implementation of their strategies. Stress-testing involves identifying possible events or changes in the external environment that could have unfavorable effects on an institution and assessing the institution's ability to withstand those effects.

9.9.7.1 Stress-testing does not necessarily mean the use of sophisticated financial modelling tools but focuses on the need for institutions to evaluate in some way the potential impact (both financial and non-financial) different stress scenarios may have on their business. The level of resources devoted to this effort should be commensurate with the nature, scale, and complexity of institutions' business activities.

9.10 Measuring and monitoring

9.10.1 The failure or success of a strategy depends on whether an institution has adequate resources and capability to implement the strategy and whether the institution can effectively monitor and control the progress of implementation. As such, in addition to strategic planning, institutions should have a process to facilitate the monitoring and control of strategies being implemented.

9.10.2 Active Board and senior management oversight with the support of the strategic risk management function will help ensure effective implementation and control of strategies. In addition, there should be adequate management guidelines and written procedures for implementing strategies and monitoring and reporting the progress of implementation.

9.10.3 Where institutions have identified strategic issues arising from anticipated operational or market changes which may result in a significant adverse impact on their business or financial conditions, such issues should be reported to the Board and senior management in a timely manner, with an assessment of the strategic risk implications and the need for taking remedial actions (such as modifying existing strategies and implementing risk mitigating or contingency measures).

9.10.4 To ensure an effective strategic risk management process, every institution should deploy a management information system that will enable management to monitor:

- Current and forecasted economic conditions, e.g., economic growth, inflation, foreign exchange trends, etc.
- Current and forecasted industry and market conditions, such as:
  - Increasing competition by new market entrants
  - Number and size of mergers and acquisitions
  - Changing customer behavior
  - New products/substitutes
- Exposure to different sectors, and associated sector risks.

9.11 Performance evaluation and feedback

9.11.1 Comparison of actual performance to desired outcomes serves as an important check on the success of implementing approved strategies and allows management to take timely remedial actions to address significant deviations from set targets. Therefore, institutions are expected to develop a performance evaluation system that tracks progress towards achieving both financial and non-financial targets.

9.11.2 To ensure efficient and continuous performance evaluation, at the setting of strategic goals and targets stage, long term goals and targets should be broken down in short term (preferably yearly) measurable goals and targets.

9.12 Specific responsibilities of senior management

9.12.1 Senior management should, among other things: –

- Establish and implement the institution's strategic risk management framework based on criteria and standards set by the Board;
- Assist the Board in developing strategies to meet the institution's strategic goals and objectives;
- Formulate the institution's strategic plan and related implementation plans (such as business, development, and operating plans)
- Ensure adequate implementation of the institution's strategic plan, as approved by the Board.
- Implement an effective performance evaluation system;
- Ensure that any strategic issues and material risks arising from environmental changes or implementation of the institution's strategies are reported to the Board on a timely basis.

9.13 Specific responsibilities for the Board

9.13.1 The Board has specific responsibilities for overseeing an institution's strategic risk management process. These includes: -

- Ensuring that the institution has in place an appropriate strategic risk management framework which suits its own circumstances, business needs and risk tolerance;
- Ensuring that the institution's strategic goals and objectives are clear and are set in line with its corporate mission and values, culture, business direction and risk tolerance;
- Approving the institution's strategic plan (including strategies contained therein) and any subsequent changes, and reviewing the plan (at least annually) to ensure its appropriateness;
- Ensuring that the institution's organization structure, culture, infrastructure, financial means, managerial resources, and capabilities, as well as systems and controls are appropriate and adequate to support the implementation of its strategies; Reviewing high-level reports periodically submitted to the Board on the institution's overall strategic risk profile;
- ensuring that any material risks and strategic implications identified from those reports are properly addressed; and
- Ensuring that senior management is competent in implementing strategic decisions approved by the Board and supervising such performance on a continuing basis.

9.14 Internal audit and controls

9.14.1 Institutions need strong internal control systems to ensure that they are not unduly exposed to strategic risks. Internal controls are required to ensure that:

- The organization structure establishes clear lines of authority.
- The institution's systems and structures provide for business continuity planning.
- The process of setting up and reviewing strategic plans is comprehensive and is adhered to.
- The results of such audit reviews, including any issues and weaknesses identified should be reported to the Board and senior management directly. Both the Board, and a delegated committee (e.g., Board Audit Committee), and senior management should be sufficiently engaged in the process to determine whether such reviews and audits are effectively performed (e.g., whether the performing staff are independent and have sufficient authority to perform their duties) and identified issues are addressed.

SECTION 9: ML/TF Risk

10.1 Principle/ definition of Risk

10.1.1 ML/ TF Risk is the risk that the CMOs activities result in its being used by criminals as a conduit to conduct money laundering and financing of terrorism. It is unrealistic to expect an organization to operate in a completely risk-free environment in terms of ML/TF. Therefore, an organization should identify the ML/TF risks it may reasonably face, then assess the best approach to reduce and manage those risks.

10.1.2 CMOs should be able to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified and would enable them to make decisions on how to allocate their own resources in the most effective way. CMOs should have in place processes to identify, assess, prioritize, monitor, manage and mitigate money laundering and terrorist financing risks. Where there are higher risks, CMOs should take enhanced measures to manage and mitigate those risks; and, correspondingly, where the risks are lower, simplified measures may be permitted by the Commission. Simplified measures will not be permitted whenever there is a suspicion of money laundering or terrorist financing.

10.1.3 Inherent ML/TF risk may fall into the following categories:

1. Products, services, and transactions;
2. Customers;
3. Countries or geographic locations; and
4. Delivery channels

10.2 Drivers of Risk

10.2.1 Key risks/ drivers of ML/ TF risk within the above categories are as follows:

1. Higher-Risk Products, Services and Transactions
   - Complex products and services e.g., derivatives
   - Significant volumes of electronic payments, such as electronic and mobile money payment systems, wire transfers, EFT, prepaid cards, and remittances;
   - CMO's customers actively engage in electronic banking services, such as remote deposit capture, online account opening, and/or Internet transactions;
   - CMO provides services to third-party payment processors or senders.
   - Use of correspondent banks and agents
2. Higher-Risk Customers
   - Significant portfolio of cash-intensive business customers, such as SMEs, marketeers, convenience stores, liquor, or retail stores.
   - CMO's customer base includes foreign entities and/or individuals
   - CMO has significant business relationship with non-bank financial institutions, including relatively new/ unregulated businesses such as casinos.
   - Significant number of professional service provider customers, including law firms, accountants, real estate brokers, etc.
   - CMO customer base includes domestic and/or foreign non-governmental organizations
   - CMO customer base includes politically exposed persons and high net worth individuals.

- If CMO deals with foreign clients, the origin/residence of those clients

3. Higher-Risk Countries or geographic locations
   - Extent to which the CMO's customers engage in or process transactions involving international locations identified by the Financial Action Task Force, or other international bodies as having strategic deficiencies in their countries' AML frameworks or being susceptible to corruption, and/or geographic locations outside of our normal business area;
   - CMO's customers located in, or conduct transactions with, offshore financial centers
   - CMO maintains branches in or have significant customer populations located within domestic locations designated as High Intensity Drug Trafficking Areas and/or High Intensity Financial Crimes Areas

10.3 Practical steps and guidance for the CMOs on managing the ML/ TF Risk

10.3.1 A CMO should conduct

- ML/TF risk assessments and profiling on its clients during onboarding and on a continuous basis during the business relationship
- ML/TF risk assessment of products and services before being offered to the public. CMO should also come up with mitigants to the identified ML/TF risks.
- KYC and client onboarding procedures
- Enhanced due diligence on high-risk clients e.g., high net worth individuals and politically exposed persons
- Simplified KYC on low-risk clients, subject to the Commission approval
- Periodic relevant AML/CFT training

10.3.2 Develop a Suspicious/Cash Transaction Reporting Framework

10.3.3 Conduct sanctions screening at onboarding and periodically

10.4 Role of Oversight Functions in managing the ML/TF Risk

10.4.1 *Role of Risk Management Function* – Develop an ML/TF risk assessment framework and undertake ongoing ML/TF risk identification, assessment, prioritization, management, and mitigation reviews.

10.4.2 *Role of the Compliance Function* – Compliance Officer to be the focal point person for AML/CFT issues and should conduct periodic compliance reviews and training. The Compliance Officer should also be the one to receive suspicious transaction reports from staff, investigating/analyzing and transmitting to the FIC.

10.4.3 *Internal Audit* – conduct periodic independent testing of the CMO's AML/CFT programme

10.5 Role of Senior Management (SM)

- Ensure that there are adequate and sufficient internal controls in place to guarantee adherence to AML/CFT programme
- designate a suitably qualified and experience AML/CFT Compliance Officer who should be at senior management level

10.6 Role of Board of Directors

- A CMO must have AML/CFT and Customer Identification Policies

- The Policies should be approved by the Board
- The Policies should be kept up to date
- ML/TF risks should periodically be discussed at Board meetings

APPENDIX I
SECURITIES AND EXCHANGE COMMISSION
CHECKLIST FOR REVIEW AND APPROVAL ADVERTISEMENTS

[Please Complete this assessment and submit it together with the request for approval under the Securities (Collective Investments Schemes) Rules and the Securities (Advertisements) Rules.]

PART 1 – REQUIREMENTS OF THE COLLECTIVE INVESTMENT SCHEME RULES

CLAUSE/ REQUIREMENTS OF THE SCHEDULE TO THE CIS RULES	COMMENTS
Commission to approve advertisements **58. (**1) Advertisements and other invitations to the public in Zambia to invest in a scheme, including public announcements, shall be submitted to the Commission for approval prior to their issue or publication in Zambia. (2) Any publication submitted for approval which concerns the trustee shall be accompanied by its written consent. (3) The approval so granted may be varied or withdrawn by the Commission as it deems fit. (4) Once authorized, the advertisement may be used for a maximum period of six months, provided there are no material changes in that period to the scheme or to the advertisement itself. (5) Unless the Commission disapproves submitted material within fourteen calendar days of its submission, the Commission shall be deemed to have approved it.	
Statements as to authorization of scheme	

59. (1) If a scheme is described as having been authorized by the Commission it shall be stated that, in giving this authorization, the Commission does not take responsibility for the financial soundness of the scheme or for the correctness of any statements made or opinions expressed in this regard. (2) Such a statement shall comply with the requirements of clause *sixty-two*.	
Mention of unauthorized schemes **60.** Advertisements and other invitations to the public in Zambia shall not refer to any scheme which has not obtained authorization from the Commission.	
Warning statements **61.** Advertisements shall include a warning statement that- (*a*) the price of units or shares, and the income from them (if the scheme pays a dividend), may go down as well as up; and (*b*) Investors are reminded that in certain circumstances their right to redeem their units or shares may be suspended.	
Format of warning statements **62. (**1) Warning statements shall be printed in type of the same size as the rest of the text in the advertisement.	

(2) Notwithstanding subclause (1), they may be in smaller text if printed in bold type or prominently outlined. (3) In all cases the warning shall be capable of being read with reasonable ease by anyone scanning the advertisement.	

PART 1 – REQUIREMENTS OF THE SCHEDULE TO THE ADVERTISEMENTS RULES

REQUIREMENTS OF THE SCHEDULE TO THE ADVERTISEMENTS RULES	COMMENTSS
Prominence of required statements **1.** The significance of any statement or other matter required by the provisions of this Schedule to be included in an advertisement shall not be disguised either through lack of prominence in relation to the remainder of the advertisement or by the inclusion of matter calculated to minimize the significance of the statement or the other matter required to be included.	
Advertisements to be clear and not misleading **2. (**1) The content of a securities advertisement and the manner of its presentation shall be such that the advertisement is not likely to be misunderstood. (2) A securities advertisement shall not contain any statement, promise, or forecast unless the licensee issuing it has taken all reasonable steps to ensure that each such statement, promise or forecast is not misleading in the form or context in which it appears.	

(3) A securities advertisement shall not contain any statement, purporting to be a statement of fact that the licensee issuing it does not believe at the time, on the basis of evidence of which he has a record in his possession, to be true. (4) If the securities or securities business to which an advertisement relates is available in limited quantities, or for a limited period or on special terms for a limited period, the advertisement may say so but, if that is not the case, the advertisement shall not contain any statement or matter that implies it is so.	
Advertisements to be distinguished from other matter **3. (**1) The terms of a securities advertisement and the manner of its presentation shall be such that it appears to be an advertisement issued with the object of promoting the securities, securities business, or licensee to which it relates. (2) Where the medium in which the advertisement is carried contains or presents other matter the advertisement shall be distinguished from that other matter so that the part that is an advertisement clearly appears as such.	
Advertisements to identify the securities or securities business to which they relate **4.** Except in the case of a short form advertisement or an image advertisement, the nature of the securities or securities business to which the advertisement relates shall be clearly described.	
Promotions to be genuine **5.** No securities advertisement shall be issued with the intention not of persuading persons who respond	

to the advertisement to pursue the subject matter of the advertisement but, with the intention instead, of persuading them to enter into an agreement, or use business services, of a description not mentioned in the advertisement.	
Advertisements not to imply governmental approval **6.** A securities advertisement shall not contain any matter that states or implies that the securities or securities business which is the subject of the advertisement or any matter in the advertisement has the approval of any Government department or of the Commission.	
Synopses to be fair **7.** A securities advertisement that states some only of the rights and obligations attaching to an investment in securities or some only of the terms and conditions of a securities agreement shall- (*a*) state sufficient of them to give a fair view of the nature of the investment in securities, of the financial commitment undertaken by an investor in acquiring the investment in securities and of the risks involved; and (*b*) state how a written statement of all of them can be obtained.	
Comparison with other investments or services **8.** A securities advertisement shall not compare or contrast one investment in securities with an alternative investment, or one securities service with an alternative securities service, unless the comparisons and contrasts are fair in relation to what	

is promoted and to the alternative having regard to what is not stated as well as to what is stated.	
Taxation **9. (**1) A securities advertisement that refers to taxation shall contain a warning that the levels and bases of taxation can change. (2) A securities advertisement that contains any matter based on an assumed rate of taxation shall state what that rate is. (3) A securities advertisement that refers to reliefs from taxation- (*a*) shall state that the reliefs are those that currently apply; and (*b*) shall contain a statement that the value of a relief from taxation depends upon the circumstances of the taxpayer.	
Cancellation rights **10.** Where a securities advertisement states that an investor who enters into an investment agreement to which the advertisement relates will be given an opportunity to cancel the agreement, the advertisement shall define the period during which the investor will have that right and the time when the period will begin.	
Past performance **11.** A securities advertisement shall not contain information about the past performance of securities investments of any description unless-	

(*a*) it is relevant to the performance of the securities investment the subject of the advertisement; (*b*) except where the source of the information is the advertiser itself, the source of the information is stated; (*c*) if the whole of the information is not set out- (i) what is included is not unrepresentative, unfair, or otherwise misleading; and (ii) the exclusion of what is excluded does not have the effect of exaggerating the success of performance over the period to which the information that is included relates; (*d*) if the information is presented in the form of a graph or chart, no part of the information is omitted so as to give a misleading impression of the rate at which variable quantities have changed; (*e*) in the case of an advertisement of units or shares in a collective investment scheme, any comparison made between the value of an investment in those units or shares at different times is on an offer to bid basis, that is to say, on the basis of what it would have cost to acquire an amount of the units at the earlier time and what a disposal of that amount of those units would have realized at the later time, and the fact that that is the basis of the comparison is stated; (*f*) the period which is selected as illustrating past performance is a period of not less than three years which period must end no more than three months before the date of the issue of the advertisement; and (*g*) the advertisement contains a warning that the past is not necessarily a guide to the future.	

Indications of the scale of business activities **12. (**1) A securities advertisement shall not contain any statement indicating the scale of the activities or the extent of the resources of a licensee, or of any group of which the licensee is a member, to imply that the resources available to support the performance of the licensee's obligations are greater than they are. (2) Statements which relate to resources of members of a group other than the licensee shall clearly state that fact.	
Risk warnings **13. (**1) This paragraph applies to any securities advertisement that is not a short form or image advertisement. (2) An advertisement shall contain a statement in accordance with this paragraph warning of the risks involved in acquiring or holding the securities investment the subject of the advertisement. (3) Where the advertisement relates to a securities investment in the case of which deductions for charges and expenses are not made uniformly throughout the life of the investment but are loaded disproportionately onto the early years, the advertisement shall draw attention to that fact and that accordingly, if the investor withdraws from the investment in the early years, he may not get back the amount he has invested. (4) Where the advertisement relates to an investment that can fluctuate in value in money terms, the statement shall draw attention to that fact and to the fact that the investor may not get back the amount he has invested.	

(5) Where the advertisement offers an investment as likely to yield a high income or as suitable for an investor particularly seeking income from his investment, the statement shall draw attention to that fact that income from the investment may fluctuate in value in money terms. (6) Where the advertisement relates to an investment denominated in a currency other than that of the country in which the advertisement is issued, the advertisement shall draw attention to the fact that changes in rates of exchange between currencies may cause the value of the investment to diminish or to increase. (7) Where the advertisement contemplates the investor entering pay unspecified additional amounts later, the statement shall draw attention to the fact that the investor may or, as the case may be, will have to pay more money later and that accordingly a transaction in that investment can lose the investor more than his first payment. (8) Where the advertisement relates to an investment that is not readily realizable- (*a*) if the investment is not traded on an established securities exchange, the statement shall draw attention to the fact that there is no established market for investment so that it may be difficult for the investor to sell the investment or for him to obtain reliable information about its value or the extent of the risks to which it is exposed; or (*b*) if the investment is traded on an established securities exchange but is dealt in so irregularly or infrequently- (i) that it cannot be certain that a price of that investment will be quoted at all times; or (ii) that it may be difficult to effect transactions at any price that may be quoted;	

the statement shall draw attention to that fact.	
Guaranteed returns **14.** A securities advertisement shall not describe a prospective investment return as being in any way guaranteed, secured, assured, or promised, either expressly or impliedly, unless the advertisement has been approved in writing by the Commission prior to its issue.	
Dating **15. (**1) Each securities advertisement in a publication shall state in the bottom right-hand corner of the advertisement the date on which it was first issued. (2) Any securities advertisement by way of a prospectus, brochure, handout, or similar marketing literature shall state the date on which it was first issued on either the front or back outside cover page. (3) Any securities advertisement by way of a cinematograph film, video or TV broadcast shall bear the date on which it was first issued prominently at the beginning or end of the advertising material.	