ANTI MONEY LAUNDERING (AML),

&

COMBATING FINANCING OF TERRORISM (CFT),

POLICY

Contents

REFERENCES

Kenya

- Capital Market Authority Guidelines on the Prevention of Money Laundering in the Capital Markets
- Proceeds of Crime & Anti-money Laundering Act, 2009
- Proceeds of Crime & Anti-money Laundering Regulations, 2013
- Prevention of Terrorism Act, 2012
- Prevention of Fraud (Investments) Act
- Anti-Corruption and Economic Crimes Act
- Counter-Trafficking in Persons Act
- Diamond Industry Protection Act
- Ethics and Anti-Corruption Act
- International Crime Act
- Narcotic Drugs and Psychotropic Substances Control Act
- National Crime Research Centre Act

Tanzania

- AML Act 2006 (Tanzania Mainland)
- Proceeds of Crime and AML Act 2009 (Zanzibar)
- AML Regulations 2012
- Bank of Tanzania (BOT) Foreign Exchange Regulations 1998 & 2003
- Proceeds of Crime act 1999 (Tanzania mainland)
- Prevention of Terrorism act 2002

Uganda

- The Financial Institutions (Anti Money Laundering), Regulation 2010
- The Draft Anti-money laundering Bill

International Standards

- FATF Recommendations, Revised February 2012
- International Standards and guidelines, including Regulatory Sanctions as applicable

DOCUMENT HISTORY

Document Name	Centum KYC/AML/CFT
Version	CAML/2014/V1

Reviewed and Recommended By:	
Graduate Trainee	14th January, 2014
Risk Analyst	16th January, 2014
Senior Risk & Compliance Officer	17th January, 2014
Legal and Tax Officer	20th January, 2014
Director, Corporate Affairs & Company Secretary	12th February, 2014

1.0 Introduction

The AML & CFT Policy is aimed at preventing the Centum Group from being used intentionally or unintentionally, by criminal elements for money laundering or terrorist activities. The AML & CFT Policy and KYC Procedures enable Centum to understand its customers and their financial dealings better which in turn helps the Group to manage the risks prudently.

For the purposes of this policy:

1. "**Centum" and/or "Group" shall represent the Centum Group i.e. Centum Investment Company Limited and all its subsidiaries whether established within Kenya or in a foreign country.**

2. A **"Business Relationship"** is any arrangement between Centum and a customer, the purpose of which is to facilitate the carrying out of transactions between the parties on a one-off, frequent, habitual or regular basis, and where the monetary value of dealings in the course of the arrangement is not known or capable of being ascertained at the outset.

   The signing of an Investment management agreement with Centum shall therefore be treated as forming a "business relationship" i.e. there shall be a business relationship between any person connected to Centum through a financial transaction who can pose significant reputational or other risk to Centum including Centum Agents. Financial transactions shall include domestic and international money transfer services such as mobile phone financial services, Western Union, etc.

3. A **"One off transaction"** means any transaction carried out other than in the course of a business relationship. For example, a single foreign currency transaction for a customer who does not have an ongoing business relationship with Centum constitutes a one off transaction.

4. "**Money Laundering**" means engagement of a person or persons, directly or indirectly in conversion, transfer, concealment, disguising, use or acquisition of money or property known to be of illicit origin and in which such engagement intends to avoid the legal consequence of such action. Money laundering is the criminal practice of processing ill-gotten gains or "dirty" money, through a series of transactions. In this way the funds are "cleaned" so that they appear to be proceeds from legitimate activities. It is also the process of changing the identity of illegally obtained money by channelling it through Centum so as to conceal the source. Refer to Annexure III: Sources of Money Laundering.

   Money laundering further means the act of a person (natural or legal entity) who:

   a) Engages, directly or indirectly, in a transaction that involves property that is the proceeds of any unlawful activity;

   b) Acquires, receives, possesses, disguises, transfers, converts, exchanges, carries, disposes, uses, removes from or brings into Kenya proceeds of any unlawful activity; or

   c) Conceals, disguises or impedes the establishment of the true nature, origin, location, movement, deposition, title of, rights with respect to, or ownership of, proceeds of any

unlawful activity where –

- (As may be inferred from objective factual circumstances, the person knows or has reason to believe, that the property is proceeds from any unlawful activity, or
- In respect of the conduct of a natural person, the person without reasonable excuse fails to take reasonable steps to ascertain whether or not the property is proceeds from any unlawful activity.

5. **"Proceeds of Crime"** means any property or economic advantage derived or realized, directly or indirectly, as a result of or in connection with an offence irrespective of the identity of the offender and includes, on a proportional basis, property into which any property derived or realized directly from the offence was later successively converted, transformed or intermingled, as well as income, capital or other economic gains derived or realized from such property from the time the offence was committed.

6. **"Predicate Offense"** A money laundering predicate offense is the underlying criminal activity that generates proceeds, which when laundered, results in the offense of money laundering. Examples of predicate offenses include drug trafficking under the law for the time being relating to narcotic drugs and psychotropic substances, terrorism including terrorist financing, illicit arms trafficking, participating in organized criminal group and racketeering, trafficking in human beings and smuggling immigrants, sexual exploitation including sexual exploitation of children, illicit trafficking in stolen or other goods, all corruption and related offences, counterfeiting of currency or goods, armed robbery, theft, kidnapping, illegal restraint and hostage taking, smuggling, extortion, forgery, piracy, piracy, hijacking, insider dealing and market manipulation, illicit trafficking or dealing in human organs and tissues, poaching, tax evasion, illegal fishing, illegal mining, fraud and other related offenses, murder, grievous bodily harm, pyramid and other similar schemes, piracy of goods, environmental crimes and any other offenses as the Minister may by notice publish in the Gazette, whether committed within or outside the boundaries of Kenya.

7. **"Terrorist"** refers to any natural person who (i) commits or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and wilfully (ii) participates as an accomplice in terrorist acts (iii) organizes or directs others to commit terrorist acts or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of Centum to commit a terrorist act.

8. **"Terrorist Act"** refers to any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or abstain from any act.

9. **"Terrorist Organization"** refers to any group of terrorists that (i) commits or attempts to commit terrorist act acts by any means, directly or indirectly, unlawfully and wilfully (ii) participates as an accomplice in terrorist acts (iii) organizes or directs others to commit terrorist acts or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist acts or with the knowledge of the intention of Centum to commit a terrorist act.

10. **"Terrorist Financing"** is the financing of terrorist acts, and of terrorists and terrorist organizations OR the provision of or making available such financial or other related services to a terrorist, group or entity which is concerned with terrorist acts, OR entering into or facilitating directly or indirectly any financial transaction directed to a dealing in property owned or controlled by or on behalf of any terrorist or entity owned or controlled by a terrorist.

11. **"Reporting Person"** means financial institutions, legal professionals, pension funds managers, securities market intermediaries, financial leasing entities, microfinance institutions, and financing housing companies, auctioneers and any other person who the Minister may appoint, by notice published in the Gazette.

12. **"Listed"** means a person, group of persons or organizations and specified entities that have been designated by the UN Security Council 1267 Committee by accessing the UN website (**http://www.un.org/Docs/sc/committees/1267/1267ListEnt.htm**) OR other specially designated nationals and blocked persons as listed by the Office of Foreign Assets Control (OFAC) on the OFAC websites.

1.1 Objectives of the AML & CFT Policy

The objective of the AML & CFT Policy is to ensure that the products and services of the Centum Group are not used to launder the proceeds of crime and that all of Centum's staff are aware of their obligations and the need to remain vigilant in the fight against money laundering/terrorist financing.

The document also provides a framework to comply with applicable laws, Regulatory guidelines specifically related with the detection and reporting of suspicious activities.

The KYC Procedures on Investment account Opening must be read in conjunction with the AML and CFT Policy. All Cadres of Staff in the Group are expected to be familiar with the contents of the document and compliance is Mandatory. Increased vigilance by Management and staff will protect Centum from the following risks:

- Adverse publicity, loss of public confidence, and loss of business.
- Financial losses that may arise as a result of fraudulent activities of the criminals.
- Confiscation by the court of the assets of drug traffickers, terrorists and other criminals..
- Legal action against the Centum Group for its role in facilitating the laundering of money.

1.2 Scope

This policy is applicable to Centum as a group. All Centum staff must therefore comply with the prescriptions of this policy. The scope of this policy shall also extend to Agents and Sub-Agents that include brokers, custodians and other service providers recruited by Centum under any guidelines in force at the time.

This policy highlights the methods of:

I. Prudent Customer identification and Verification of Customer's Identity

II. Establishment and Maintenance of Customers Transaction Records, Investment account Files and Business Correspondence
III. Identification and Reporting of Suspicious activities/transactions to the appropriate authorities for further investigative actions.

The subsidiaries of the Centum Group shall endeavour to comply with this Policy and where there is conflict between the Policy and the regulatory requirements of the host country; the more stringent requirement should be adopted to the extent that it is permitted by the host country's laws and regulations.

1.3 Responsibility of Board of Directors

It is the responsibility of the Centum Board of Directors (BOD) to establish appropriate anti-money laundering policies and procedures and to train staff to ensure adequate identification of customers, source of funds and the use of the said funds. Such policies should also ensure the effective prevention, detection and control of possible money laundering and terrorism financing.

The Board shall ensure that:

a) Centum has in place a Board approved Anti-Money Laundering and Combating Financing of Terrorism Policy which is consistent with the law and which shall among other things, provide for:

- Empowerment of the duly appointed Money Laundering Reporting Officer (MLRO) Officer with the necessary authority and resources to carry out the function
- Monitoring and control of Money Laundering and Financing of Terrorism risks at the highest level
- Training of staff on AML/CFT issues-i.e. identification of customers, source of funds and the use of the said funds etc.
- Customer identification procedures in line with law and implementing regulations
- Record keeping in accordance with law and implementing regulations
- Know Your Customer (KYC) and Customer Due Diligence (CDD)
- Enhanced Due Diligence in the case of large, complex or unusual transactions and transactions of Politically Exposed Persons (PEPs)
- Internal policies/procedures and controls, including appropriate compliance management arrangements, and adequate screening procedures to ensure high standards when hiring employees
- Risk management or internal audit function to test the consistency and robustness of the system
- Monitoring and reporting of suspicious transactions that may indicate money laundering or other attempts to conceal the true identity of customers or ownership of assets to the Financial Reporting Centre (FRC).

b) Centum cooperates with national law enforcement agencies by taking appropriate measures which are consistent with the law where there are reasonable grounds for suspecting money laundering.
c) The subsidiaries are aware of the reporting requirements as directed by the CBK / FRC with regard to suspicious transaction reporting and sanctions reporting.
d) Centum's anti-money laundering desk has adequate staff strength necessary for effective discharge of their responsibilities

1.4 Responsibility of Senior Management

a) Ensuring that an effective AML Program that addresses the risks posed by money launders and enhances the ability of Centum to identify, monitor, and deter persons from attempting to gain access to, or make use of the financial system is in place and that it is implemented in letter and spirit.
b) Ensuring that the program is documented and establishes clear responsibility and investment accountability to ensure that policies, procedures and controls are introduced and maintained.
c) Provide for and document policies and procedures to perform independent testing / audit, to measure compliance with the relevant AML laws and regulations.
d) Provide for and document AML training for appropriate personnel.
e) Provide for adequate screening policies and procedures to ensure high ethical and professional standards when hiring staff.
f) Ensuring that the Senior Risk Officer is promptly advised where there are reasonable grounds to know or suspect that transactions or instructions are linked to criminal conduct, money laundering or terrorist financing.
g) Centum maintains a register of all reports made to the MLRO and FRC.

1.5 Responsibility of Senior Risk Officer & Compliance

a) The Senior Risk Officer & Compliance shall act as the Group's Money Laundering Reporting Officer (MLRO).
b) Ensure that Centum has procedures for monitoring compliance as well as the effectiveness of AML Policies and procedures which must be clearly laid down in the form of policy documents and internal procedural manuals;
c) Ensure that the internal policies, procedures, and controls are based upon Centum's money laundering risk assessment;
d) Shall be the central point of contact with the Financial Reporting Centre / Correspondent financial institutions and other regulators for anti-money laundering purposes;
e) Receive and vet suspicious activity reports from staff;
f) File suspicious transaction reports with Financial Reporting Centre;
g) Develop Centum's AML compliance programme;
h) Ensure that the AML compliance programme is followed and enforced within Centum;
i) Coordinate training of staff in AML awareness, detection methods;
j) Maintain close cooperation and liaison with the Regulators and Financial Reporting Centre;
k) Ensure that Centum's controls with respect to "Know your employee" are enforced to deter internal fraud and abuse by ensuring that all the Staff within the institution:

I. Follow a code of ethics
II. Avoid and disclose conflicts of interest
III. Maintain good credit ratings
IV. Adhere to policies on rotation of duties and mandatory vacations
V. Require the use of employee identification cards for access to secure areas.

Employees who wilfully neglect to perform official duties or engage in careless or improper performance of any work in one's line of duty which results to violation of any of the Regulations of Centum's AML and CFT policy and Investment account Opening Procedures engages in gross misconduct which may result in summary dismissal or even persecution in a court of law. Kindly refer to the Human Resources Policy on Disciplinary Rules and Procedures which can be accessed on Centum's info under the HR Folder for further guidance.

2.0 Methodology

2.1 Money Laundering

DEFINITION: Money laundering is the criminal practice of processing ill-gotten gains or "dirty" money, through a series of transactions. In this way the funds are "cleaned" so that they appear to be proceeds from legitimate activities. It is also the process of changing the identity of illegally obtained money by channelling it through the Group so as to conceal the source. Refer to Annexure II: Sources of Money Laundering.

The Proceeds of Crime and Anti-Money Laundering Act 2009

- Criminalizes money laundering
- Provides for both criminal and civil restraint, seizure and forfeiture
- Places an obligation on financial institutions to:

I. Monitor and report suspected money laundering activity
II. To verify customer identity (KYC)
III. To establish and maintain customer records
IV. To establish and maintain internal reporting procedures

- Establishes the Financial Reporting Centre (Financial Intelligence Unit), the Asset Recovery Centre and the Criminal Assets Recovery Fund
- Provides for procedures that facilitate international assistance with investigations and proceedings related to money laundering offences.
- The Proceeds of Crime and Anti-Money Laundering Act, 2009, makes it an offence for any person to enter into an agreement or engage in any arrangement or transaction with anyone in connection with property that forms part of the proceeds of crime, whether that agreement, arrangement or transaction is legally enforceable or not and whose effect is to:

I. Conceal or disguise the nature, source, location, disposition, movement or ownership of the said property;
II. Enable or assist any person who has committed or commits an offence, whether in Kenya or elsewhere to avoid prosecution; or
III. Remove or diminish any property acquired directly, or indirectly, as a result of the commission of an offense.
IV. Acquire proceeds of a crime or assist anyone whom they know or suspect has committed, or benefited from any criminal conduct. (Acquire, Possess & Assist)
V. Prejudice an investigation by informing the subject of a suspicion, or any third party that a disclosure has been made either internally or externally, or that the authorities may act or propose to act or investigate. (Tip off)
VI. Acquire knowledge or a suspicion, or has reasonable grounds to know or suspects, that benefit has been gained from criminal conduct or that the proceeds of crime have been laundered, and have not been reported as soon as possible. Centum staff negligent in this respect would be liable for prosecution. (Failure to report)
VII. Failure to put in place systems, controls and procedures to guard against money laundering. (Systems and Controls)

- It is an offence for an institution to fail to:
  I. Monitor and report suspected money laundering activity
  II. Verify customer identity
  III. Establish and maintain customer records.

The Act accords immunity or protection to institutions and officers in respect of obligations done under the Act in good faith such as reporting of suspicious transactions.

If any staff is aware or suspects that a transaction or instruction is related to any crime, he/she must report the transaction to the Senior Risk Officer even if he/she is not handling the transaction, instruction or funds in question.

2.2 Stages of Money Laundering

The first step in the laundering process is for criminals to attempt to get the proceeds of their crimes into an investment company or other financial institution, sometimes using a false identity. They can transfer the proceeds to other investment accounts, locally or abroad, or use it to buy other goods or services. It eventually appears to be like any legally earned money and becomes difficult to trace back to its criminal past. The criminals can then invest or spend it or, as is often the case, use it to fund more crime.

Money laundering usually takes place in three stages as described below:

1. **Placement (Injection or Pre-washing)**

The physical disposal of the initial proceeds derived from illegal activity. Placement is the means by which funds derived directly from a criminal activity are introduced into the financial system either directly or using other retail businesses. This can be in the form of large sums of cash or a series of smaller sums. Initial proceeds of drug trafficking or street sales of drugs are always in cash. Placement techniques include the following:

a) Smurfing: Involves the deposit of small amounts of illegal cash into investment account(s). Typically, smurfing deposits are in small amounts in order to avoid Regulatory requirements of reporting cash transactions.
b) Alternative Remittances: It refers to the transfer of funds through "alternative" or illegal money transfer systems. These systems are unregulated and illegal, but they are used to transfer both legitimate and illegal funds. Alternative Remittances are also known as underground or parallel banking. There are very large networks of these systems in operation around the world.
c) Electronic Transfers: In the money laundering context, an electronic transfer involves the transfer of money through electronic payment systems that do not require sending funds through a bank account. If the amount is below the CTR (Cash Transaction Reporting) limit then it will not be reported as per prevailing regulations.
d) Asset Conversion: Asset Conversion simply involves the purchase of goods. Illegal money is converted into other assets, such as real estate, diamonds, gold and vehicles, which can then be sold and proceeds can be deposited in the investment account.
e) Bulk movement: Involves the physical transportation and smuggling of cash and monetary instrument such as money orders and cheques.
f) Securities Dealing: Illegal funds are placed with securities firms and used for buying bearer

securities and other easily transferable instruments.

2. **Layering (Staking or Washing)**

Separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity. The aim is to disguise the transaction through a succession of complex financial transactions with the purpose of erasing as quickly as possible all links with its unlawful origin. The funds may be converted into shares, bonds or any other easily negotiable asset or may be transferred to investment accounts in other jurisdictions. Other techniques and institutions that can facilitate layering include the following:

a) Offshore banks: Offshore Banks accept deposits from non-resident individuals and corporations. A number of countries have well-developed offshore banking sectors; in some cases combined with loose anti-money laundering regulations.
b) Shell corporations: A shell corporation is a company that is formally established under applicable corporate laws, but does not actually conduct a business. Instead, it is used to engage in fictitious transactions or hold investment accounts and assets to disguise their actual ownership.
c) Trusts: Trusts are legal arrangements for holding specified funds or assets for a specified purpose. These funds or assets are managed by a trustee for the benefit of a specified beneficiary or beneficiaries. Trusts can act as layering tools as they enable creation of false paper trails and transactions. The private nature of trusts makes them attractive to money launders.
d) Walking Investment accounts: A walking investment account is an investment account for which the investment account holder has provided standing instructions that upon receipt all funds should be immediately transferred into one or more investment accounts. By setting up a series of walking investment accounts, criminals can automatically create several layers as soon as any fund transfer occurred.
e) Intermediaries: Lawyers, investment accountants and other professionals may be used as intermediaries or middlemen between the illegal funds and the criminal. Professionals engage in transactions on behalf of a criminal customer who remains anonymous. These transactions may include use of shell corporations, fictitious records and complex paper trails.

3. **Integration (Recycling)**

The provision of apparent legitimacy to criminally derived wealth. If the layering process has succeeded, an integration scheme places the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing as normal business funds. Complex integration schemes place the laundered funds back into the economy through real estate, business assets, securities and equities, in such a way that they appear to have been legitimately earned. Various integration techniques include:

a) Import / Export transactions: To bring illegal money into the criminal's country of residence, the domestic trading company will export goods to the foreign trading company on an over-invoiced basis. The illegal funds are remitted and reported as export earnings. The transaction can work in the reverse direction as well.
b) Business Recycling: Legitimate businesses also serve as conduits for money laundering. Cash-intensive retail businesses, real estate, jewellers, and restaurants are some of the most traditional methods of laundering money. This technique combines the different stages of the money laundering process.
c) Asset Sales & Purchases: This technique can be used directly by the criminal or in combination with shell corporations and corporate financings. The end result is that the criminal can treat the

earnings from the transaction as legitimate profits from the sale of the real estate or other assets.

d) Consultants: The use of consultants in money laundering schemes is quite common. The consultant could be fake. For example, the criminal could himself be the consultant. In this case, the criminal is channelling money back to himself. This money is declared as income from services performed and can be used as legitimate funds.

e) Credit & Debit Cards:

- Credit cards: Are an efficient way for launders to integrate illegal money into the financial system. By maintaining an investment account in an offshore jurisdiction through which payments are made, the criminal ensures there is a limited financial trail that leads to his country of residence.
- Debit cards: Individuals first transfer illegal funds into an offshore investment account and signs up for a debit card from the bank to utilize the funds.

f) Corporate Financing: Corporate financings are typically combined with a number of other techniques, including use of offshore banks, electronic funds transfers and shell companies.

The three basic steps may occur as separate and distinct phases. Alternatively, they may occur simultaneously or, more commonly, they may overlap. How the basic steps are used depends on the available laundering mechanisms and the requirements of the criminal organization.

3.0 Terrorist Financing

Terrorist Financing can be defined as the financial support, in any form, to terrorism or of those who encourage, plan, or engage in terrorism. A terrorist group, like any other criminal organization, builds and maintains an infrastructure to develop sources of funds and channel them to those who provide materials and or services to the terrorist organization.

A "Terrorist Act" means an act or threat of action which:

a) Involves the use of violence against a person
b) Endangers the life of a person, other than the person committing the action
c) Creates a serious risk to the health or safety of the public or a section of the public
d) Results in serious damage to property
e) Involves the use of firearms or explosives
f) Involves the release of any dangerous, hazardous, toxic or radioactive substance or microbial or other biological agent or toxin into the environment
g) Interferes with an electronic system resulting in the disruption of the provision of communication, financial, transport or other essential services
h) Interferes or disrupts the provision of essential or emergency services
i) Prejudices national security or public safety.

Terrorist acts are carried out with the aim of:

a) Advancing a political, religious, ethnic, ideological or other cause; and
b) Causing fear amongst the members of the public or a section of the public, or intimidating or compelling the Government or an international organization to do or refrain from doing an act.

"Terrorist Group" means:

a) An entity that has as one of its activities and purposes, the committing of, or the facilitation of the commission of a terrorist act; or

b) A specified entity

"Terrorist Property" means:

a) Proceeds from the commission of a terrorist act, money or other property which has been, is being or is intended to be used to commit a terrorist act; or
b) Money or other property which has been, is being, or is intended to be used by a terrorist group.

A person who knowingly:

a) Deals directly or indirectly, in any property that is owned or controlled by or on behalf of a terrorist group;
b) Enters into, or facilitates, directly or indirectly any transaction in respect of property referred to at (a) above;
c) Provides financial or other services in respect of property referred to in paragraph (a) at the direction of the terrorist group;

Commits an offence and is liable, on conviction, to imprisonment for a term not exceeding 20years. Centum staff must thus prove that they took all reasonable actions to satisfy themselves that property is not owned or controlled by or on behalf of a terrorist group so as not to be liable in any civil action for any action taken in relation to that property.

4.0 Regulatory Oversight and Compliance Risks

The consequence of contravening the Regulations or failing to comply can be significant and include disciplinary measures, imprisonment or fine or both under local laws as well as the loss of reputation for the Centum Group. Increased vigilance by Management and the staff will protect Centum from the following risks:

a) Reputation risk: The reputation of Centum is the core of its success. The ability to attract good employees, customers, funding and business is dependent on reputation. A strong KYC/AML/CFT/CAP Policy should help the Group put in place preventive measures to avoid being used as a vehicle for illegal activities.
b) Operation risk: This is the risk of direct or indirect loss from faulty or failed internal processes, management and systems. In today's competitive environment, operational excellence is critical for competitive advantage. If KYC/AML/CFT/CAP Policy is faulty or poorly implemented, then operational resources are wasted and there is an increased chance of being used by criminals for illegal purposes. Time and money is then spent on legal and investigative actions and the business can be viewed as operationally unsound.
c) Legal risk: If Centum is used as a vehicle for illegal activity by customers, it faces the risk of fines, penalties, injunctions and even forced discontinuance of operations.
d) Financial risk: If Centum does not adequately identify and verify customer details, it may run the risk of unwittingly allowing a customer to pose as someone they are not. The consequences of this may be far reaching.

5.0 Know Your Employee (KYE) Policy

Centum shall institute specific "know your employee" controls designed to deter internal fraud and abuse of the institution which require employees to:

a) Follow a code of ethics;
b) Avoid and disclose conflicts of interest;
c) Maintain good credit ratings;
d) Adhere to policies on rotation of duties and mandatory vacations; and
e) Require the use of employee identification cards for access to secure areas.

6.0 Know Your Customer (KYC) Policy

"Know your customer" requirements consist of obtaining full particulars of the customer's identity and having a sound knowledge of the purpose for which the customer is seeking to establish a business relationship with Centum. In certain circumstances, the information obtained may need to be verified. The need to know Centum's customers is vital for the prevention of money laundering and underpins all other activities. The key to avoiding frauds and anti-money laundering lie in:

A. **KNOW YOUR CUSTOMER**
- Customer identity and background
- Beneficial owner and background
- Source of funds
- Monitoring over time

B. **KNOW YOUR PROCESS**
- Policies, procedures and controls
- Roles and responsibilities

C. **KNOW YOUR TRANSACTION**
- Trace complex, large transactions
- Spot unusual behaviour
- Large volume transactions
- Look for the "needle in the haystack"

Centum has framed the KYC Policy around the five elements below:

a) Customer Acceptance Policy;
b) Customer Identification Procedures;
c) Establishment and Maintenance of Customer Records
d) Monitoring of Transactions;
e) Continuous Risk Management.

6.1 Customer Acceptance Policy (CAP)

a) No investment account shall be opened in anonymous or fictitious name(s) or on behalf of persons

whose identity has not been disclosed or cannot be verified. Kindly refer to Centum's Procedures on Investment account Opening for guidance on how to deal with exceptions in this area.

b) Centum must establish to its satisfaction that it is dealing with a person that actually exists, and identify those persons who are empowered to undertake the transactions, whether on their own behalf or on behalf of others.
c) It is imperative for all Centum staff employed in this process to be aware of the risks involved at this stage because it is the stage where, among other things, launderers may engage in direct deceit and try to hide their true identity or that of their criminal customers. For instance, launders may use false names and produce fake identity documents or attempt to hide the beneficial owners of the investment account / transactions.
d) To curb the risk, the AML Act and Prudential guidelines have prescribed information that should be obtained from customers whenever opening or initiating business relationships with them and requirements for verifying the information furnished. In this respect the following original documents must always be sighted:

Individuals / Sole Proprietors / Partners / Principal Officers of Societies & Trusts / Directors and Shareholders with more than 5% shareholding in organizations;

- Personal Identification Card (ID) / Passport
- Copy of PIN Certificate
- Bank statements for the last 6 Months
- Two (2) Passport size photos
- Letter of Introduction
- Utility Bill
- Signature Verification
- Bank Reference Letter

Corporations / Clubs / Societies / Associations

- Evidence of registration or incorporation – Certificate of registration
- The Act establishing the body corporate
- A board corporate resolution authorizing a person to act on behalf of the body corporate together with a copy of the latest annual returns submitted in respect of the body corporate in accordance with the law under which it was established;

In the case of a government department

- A letter from the investment accounting officer
- Utility bill

Non Kenyan Residents

For prospective non-Kenyan resident customers who wish to create a business relationship without face-to-face contact, it will not be practical to seek sight of a passport or national identity card. There are a number of alternative measures that shall be taken:

I. Any subsidiaries, head offices or correspondent financial institutions in the prospective client's

home country may be used to confirm identity or as an agent to check personal verification and address details

II. Where the institution has no group presence or correspondent relationship in the country of residence, a copy of the passport authenticated by an attorney, notary or consulate could be obtained; or

III. An investment account opening reference can be sought from a reputable credit or financial institution in the applicant's home country. Verification details should be requested covering true names used, current permanent address, date of birth and verification of signature.

e) When a business relationship is being established; the nature of business that the customer expects to conduct should be ascertained, so as to determine what might be expected as the client's normal activity level. In order to judge whether a transaction is or is not suspicious, Centum needs to have a clear understanding of the pattern of its customer's business as its relationship with the customer develops. Suspicious transactions may arise at any stage, and frequently occur within an established relationship rather than at the onset.

Refer to the Investment account Opening Procedures for the detailed requirements for:

- Individuals
- Body Corporate Customer

Note: Centum should have full disclosure of ultimate beneficiaries / owners / controlling persons behind nominee / trust investment accounts.

6.2 Customer Identification Procedure (CIP)

a) Centum must obtain sufficient information necessary to establish the identity of each new customer, whether regular or occasional, and the purpose for the intended nature of business relationship.

b) Centum must also be able to satisfy the competent authorities that due diligence was observed based on the risk profile of the customer in compliance with the prudential guidelines in place.

c) Centum has adopted a risk based approach. Parameters of risk perception are clearly defined in terms of the nature of business activity, location of customer and his customers, mode of payments, volume of turnovers, social and financial status etc. to enable categorization of customers into low, medium and high risk. Customers requiring very high level of monitoring e.g. PEPs may, if considered necessary, be categorized even higher.

d) Centum has put in place measures to ensure that a customer does not have multiple identities within Centum, by having in place a unique identification code for each customer. The Unique Identification Code helps Centum identify customers, track the facilities availed, monitor financial transactions in a holistic manner and enable Centum to better risk profile customers.

e) Where a customer already has an existing investment account, should the customer wish to transfer the investment account to another subsidiary within Centum, as long as full KYC has been done for the concerned customer, the customer shall be allowed to transfer his investment account from one subsidiary to another without restrictions. In order to comply with KYC requirements of correct address of the person, fresh address proof may be obtained upon such transfer by the transferee subsidiary.

f) Centum shall update customer identification data (including photographs) after the investment account is opened. The periodicity of such review shall be once every 3 years in case of low risk category customers and every 2 years for medium risk and every 1 year for high risk categories.

g) Centum shall prepare a profile for each new customer based on risk categorization. The nature and extent of due diligence shall depend on the risk perceived by Centum. Enhanced due diligence (EDD) shall be applied to persons and entities that present a higher risk. This shall be addressed with the following measures:

- Obtaining further information to establish the customer's identity;
- Applying extra measures to check documents supplied e.g. verification directly with the issuing authorities;
- Obtaining senior leadership approval for the new business relationship or transaction;
- Establish the person's / entity's sources of funds e.g. undertaking surprise site visits;
- Carry out on-going monitoring of the business relationship.

7.0 Customer Due Diligence (CDD)

While adherence to "KYC" policy is MANDATORY, adherence to CDD and procedure is essential for the safety and ethical standards of Centum's operations. Centum must be satisfied that it has adequate controls to establish the true identity of prospective customers or users of Centum's facilities and that sufficient KYC information is collected.
Based on due diligence conducted, Centum would maintain risk profiles of all its customers and would keep them up-dated. Risk profile of all prospective customers must be assessed by the subsidiary directors for money laundering purposes and the ongoing KYC and monitoring procedures will be set according to that risk.
In addition to the "KYC" policy, a measure incorporated into CDD is searching through worldwide databases for any incidences of the customer named as potential threat, or terrorist financier.

7.1 Guiding Principles for Centum

a) Do business with customers whose status and identity is fully known to Centum.
b) Determine identity and maintain risk profile, background and business records of all customers.
c) Regularly monitor relationships and keep profiles and records updated.

Centum's policy is to identify customers:

a) When establishing initial business relations
b) When undertaking occasional or one-off transactions
c) When there is cause to be suspicious
d) When there is doubt about veracity or adequacy of previously obtained identification information.
e) No remittances shall be undertaken by any subsidiary without first confirming the full names of both the originator and beneficiary against the international watch lists.

7.2 Prohibited Customer Types

As a policy, Centum does not undertake business with:

a) Anonymous customers
b) Individual or entities subject to UN / OFAC or local country sanctions

c) Shell corporations
d) Customers hiding beneficial ownership of the investment account
e) Government investment accounts in personal names of the government officials
f) Unauthorized money changers / prize bond dealers

7.3 Declining Clients

Where Centum is unable to fully comply with the customer due diligence requirements, it:

a) Shall not open the investment account, commence the business relationship or perform or undertake the transaction; or
b) In the event Centum has already commenced the business relationship, terminate the business relationship; and
c) File a suspicious transaction report in accordance with the Prudential Guidelines.

7.4 Beneficial Ownership

a) Centum shall ensure that it is able to identify and verify the natural persons behind legal persons and arrangements.
b) In addition, Centum is required to understand the nature of business, ownership and control structure when performing CDD measures in relation to customers that are legal persons or legal arrangements.
c) The objective of undertaking this function would be to identify the natural persons exercising control and ownership in the legal person or arrangement. Information that may be obtained from customers to assist institutions in this function includes the following:

    - Certificate of incorporation
    - Partnership agreement
    - Deed of Trust
    - Memorandum and Articles of Association
    - Official returns showing registered office and if different the principal place of business
    - Names of the relevant persons having senior management position in the legal person or trustees of the legal arrangement
    - Names of the trustee, beneficiaries or any other natural person exercising ultimate effective control over the trust.
    - Any other documentation from a reliable independent source proving the name, form and current existence of the customer.

d) The relevant identification data may be obtained from a public register, from the customer or other reliable sources.
e) Where a person is purporting to act on behalf of another person whether as a nominee or otherwise, Centum should ensure that it is able to identify and verify that person.

8.0 Investment account Opening Forms

a) Investment account Opening forms should be completed in full and any blank spaces should be duly cancelled out.
b) Details indicated therein should be confirmed/counter checked against other documents presented by the investment account opener and the Introducer.
c) When opening investment accounts, staff must ensure that best endeavours are undertaken to collect all relevant information, concerning connectivity to other investment accounts or customers of Centum. The information obtained, should be recorded on the Investment account Opening / KYC forms.

8.1 Introductions and References

a) Introductions are normally taken before the investment account is opened whilst References are normally sought after the investment account has been opened.
b) The purpose of taking positive introductions is to ensure that we open investment accounts for persons of good repute, integrity, and means and for persons whose intent is to genuinely utilize our various investment services and products and NOT to carry out fraudulent transactions including Money Laundering.
c) References are secondary to introductions and they serve the purpose of confirming that the persons whose investment account has been opened are indeed genuine and known to be of good character and also to confirm salient details of the person.

d) Staff members may also introduce clients; however Extreme Due Diligence (EDD) must be exercised where opening investment accounts for walk in customers.
e) Where applicable, written confirmation from customer's bank attesting to customer's identity and history of investment account relationship (bank referee).
f) For investment accounts with more than one party and where one of the parties has identified the others, written confirmation must be obtained to the effect that the first party has known the other(s) personally for at least 12 months.
g) The name and investment account number of the introducer must be captured in FCC on investment account opening.
h) Examples of references are Status reports, Registry Search reports, Bank reports and other third party but reliable confirmations.

8.2 Capacity to Introduce an Investment account

For a person to introduce another for the purposes of creating a business relationship, he/she must have capacity to do so i.e.:

- Introductions from persons of bad character, unsound minds or those who do not conduct their investment accounts properly should not be accepted.
- The potential investment account opener must be well known to the introducer.

9.0 Risk Assessment and Management

a) Centum shall undertake a Money Laundering and Financing of Terrorism Risk Assessment.
b) The Assessment shall provide the means for identifying the degree of potential money laundering and financing of terrorism risks associated with specific customers and transactions thereby allowing the institution to focus on customers and transactions that potentially pose a greater risk of money laundering and terrorism financing.
c) In addition, the risk assessment shall enable Centum to assess, monitor, manage and mitigate the risks associated with money laundering.
d) The risk assessment conducted by Centum shall enable the group to adopt a risk based approach towards managing and mitigating risks related to anti-money laundering and the financing of terrorism.
e) Centum shall undertake enhanced measures to manage and mitigate AML/CFT risks where higher risks are identified; correspondingly, where risks are lower, simplified measures may be permitted.
f) Simplified measures shall however not be undertaken whenever there is a suspicion of money laundering or terrorist financing.
g) Centum shall take into consideration the findings of the country's National Money Laundering and Terrorism Risk Assessment.
h) Centum shall update the Risk Assessment Policy annually or earlier where warranted, in order to take into investment account changes such as the entry into new markets and the introduction of new products and services.

9.1 Risk Assessment Factors

When preparing a risk assessment, Centum shall consider factors such as:

a) The number and volume of transactions per customer,
b) Nature of the customer relationships, and
c) Whether, for example, the institution's interaction with customers is face-to-face or non-face-to-face

9.2 Risk Assessment Framework

The development of the AML risk assessment framework involves three steps:

a) Identifying and assessing the money laundering and terrorism financing risks that may be associated with Centum's unique combination of products and services, customers, geographic locations and delivery channels.
b) Conducting a detailed analysis of all available data to assess the level of risk within each high risk category; and,
c) Determining whether Centum's AML compliance program is adequate and provides the necessary controls to mitigate the risks identified.

9.3 Risk Categories

9.3.1 Country Risk

a) Centum shall identify domestic and international geographic locations that may pose a higher risk to its AML/CFT compliance program.
b) Each case should be evaluated individually when assessing the risks associated with doing business, such as opening investment accounts or facilitating transactions, in certain geographic locations.
c) Factors that may result in a country or region posing a higher risk include:
   - Countries that are subject to sanctions, embargoes or similar measures issued by credible organizations such as the United Nations ('UN'), the Financial Action Task Force (FATF).
   - Countries identified by credible sources as lacking appropriate AML/CFT laws, regulations and other measures.
   - Countries identified by credible sources as providing funding or support for terrorist activities or that have designated terrorist organizations operating within them.

9.3.2 Products/Services Risk

a) Centum shall consider the potential money laundering and terrorism financing risks associated with each specific product or service prior to its introduction to the market.

b) Special attention should be paid to the risks associated with new or innovative products or services not specifically being offered by the institution, but which make use of the institution's services to deliver the product. Such products or sources could include:

- Mobile Phone Financial Services;
- Foreign exchange and funds transfers;
- Trust and asset management services;
- Monetary instruments;

9.3.3 Customers/Entities Risk

a) Centum shall determine, based on its own criteria, whether a particular customer poses a higher risk.
b) Certain customers and entities may pose specific risks depending on the nature of the business, the occupation of the customer, or the nature of anticipated transaction activity. Some factors to consider include:

I. Customers conducting their business relationship or transactions in unusual circumstances, such as:

   - Significant and unexplained geographic distance between the institution and the location of the customer;
   - Frequent and unexplained movement of investment accounts to different institutions; and;
   - Frequent and unexplained movement of funds between institutions in various geographic locations.

- Customers whose structure or nature of the entity or relationship makes it difficult to identify the true owner or controlling interests.
- Foreign financial institutions, including banks and foreign money service providers such as Forex bureaus, and money transmitters.

II. Non-bank financial institutions such as money services businesses, casinos and brokers/dealers in securities, and dealers in precious metals, stones, real estate dealers.

III. Publicly exposed persons (PEPs). Individuals who are or have been entrusted with prominent public functions (both foreign and local), for example, senior politicians, senior government officials, judicial or military officials, senior executives of state owned corporations, important political party officials. Business relationships with family members or close associates of PEPs may involve reputational risks similar to those with PEPs.

IV. Resident and Non- resident aliens (NRAs) and investment accounts held by foreign individuals.

V. Foreign corporations and domestic business entities, particularly offshore corporations such as domestic shell companies, private investment companies and international business corporations located in high-risk geographic locations.

VI. Cash-intensive businesses, including, for example, supermarkets, convenience stores, restaurants, retail stores, liquor stores, wholesale distributors

VII. Foreign and domestic non-governmental organizations and charities.

VIII. Professional service providers.

c) Centum shall make its own determination as to the risk weights to assign to the different risk. The weight assigned to each of these risk categories (individually or in combination) in assessing the overall risk of potential money laundering may depend on their respective circumstances.

9.4 Conducting a detailed Analysis on all Available Data

a) The second step of the risk assessment process entails a detailed analysis of the data obtained during the identification stage in order to assess the AML Risk. This stage involves obtaining quantitative data pertaining to the institution's activities, different weights are assigned to each product/service, customer/entity and geographical based on the following:
   - The institution's ability to identify the customer.
   - Number and volume of transactions.
   - Past history

b) Centum shall make its own determination as to the risk weights to assign to the different risk. The weight assigned to each of these risk categories (individually or in combination) in assessing the overall risk of potential money laundering may depend on their respective circumstances.

9.5 Building a Risk-Based AML Program

The third step is the process of building a risk-based AML program which adequately addresses the concerns identified in the risk assessment. This includes establishing appropriate policies and procedures to monitor and control the various risks with particular emphasis placed on those risk categories classified as "high risk".

10.0 Risk Classification

The risk posed by customers shall be assigned on the following basis:

i. Low Risk (Level I):

Individuals and entities whose identities and sources of wealth have been identified and whose transactions conform to the known profile are categorized as low-risk. Illustrative examples of low risk customers are salaried employees whose salary structures are well defined, Government Departments and Government owned companies, regulators and statutory bodies etc.

ii. Medium Risk (Level II):

For new investment accounts, where Centum has done adequate due diligence, but where it is felt that the transaction behaviour cannot be readily established, such investment accounts may be classified as medium risk for a period of six months and closely monitored. In addition, the account shall have limited transactions; the nature of which is restricted to transfers of amounts – into the account. These transfers do not include dividends, interest accrued and investment related gains or losses. This could also apply to existing investment accounts which reflect a change in investment account operations / investment account operating mandates.

iii. High Risk (Level III):

(Centum shall not establish relationships with any persons or customers that it considers high risk).
A customer / company would be considered "High risk" where Centum is not in a position to establish to its satisfaction, that it is dealing with a person that actually exists, and identify those persons who are empowered to undertake the transactions, whether on their own behalf or on behalf of others.

This also applies where Centum is not able to establish the true nature of business that the customer expects to conduct so as to determine what might be expected as the customer's normal activity level.

This also extends to areas where full disclosure of beneficial owners or controlling persons behind nominee investment accounts cannot be established.

In such situations, Centum takes an active decision not to proceed with investment account opening or other transaction. ***For investment accounts that Centum considers "High Risk", a decision shall be immediately taken not to open the investment account. For an existing investment account that changes its profile from either "low risk" or "medium risk" to "high risk", an immediate decision to terminate the relationship shall be taken***. However, where this is not immediately possible such an investment account shall be subjected to intensive monitoring. Where the investment account operation warrants reporting to the regulator, a Suspicious Activity Report shall be immediately filed.

The examples of customers requiring higher due diligence may include, but not limited to:

- Trusts, charities, NGOs, NPOs, Foundations, Welfare Association, Religious Entities, Clubs, Societies, Financial Institutions, Foreign Exchange Bureaus, Jewellers, Controversial entity and organizations receiving donations with inadequate information as to the source or why
- Politically Exposed Persons (PEPs)
- Correspondent Relationships
- Non Resident Customers

- Investment accounts of foreign nationals belonging to sanctioned / high risk / Non co-operative countries (NCCT)
- High Net worth individuals whose source of funds / investments cannot be substantiated
- Companies having close family shareholding or beneficial ownership
- Non-face to face / On-line customers,
- Persons with dubious reputation as per public information available

11.0 Legitimacy of Funds and Transactions

Note: When reviewing legitimacy of funds, the review shall focus on investment account activity (e.g. large, frequent or unusual deposits, withdrawals, payments or exchanges of cash, foreign currency or negotiable instruments) ***which is not consistent with or reasonably related to the customer's normal business activities or financial standing i.e. Out of Pattern Transactions***. The following types of information will be considered the minimum acceptable for determining the legitimacy of funds and transactions which are not consistent with the investment account pattern:

a) For large, frequent or unusual cash deposits or withdrawals - written statement from the customer confirming that the nature of his/her business activities normally and reasonably generates substantial amounts of cash;
b) For large, frequent or unusual currency exchanges - written statement from the customer confirming the reason and need for acquired currencies;
c) For multiple or nominee investment accounts, or similar or related transactions - written statement from the customer confirming the reason and need for multiple or nominee investment accounts, or similar or related transactions;
d) For large, frequent or unusual transfers or payments of funds - appropriate documentation as to the identity of the recipient (or sender) of the transferred or paid funds, and the reason underlying the transfer or payment;
e) For large or unusual investments or requests for advice or services - written statement from the customer confirming that the investments or advice or services being requested are bona fide and consistent with the goals and objectives of the customer's reasonable and normal business activities;
f) For large or unusual foreign transactions - written confirmation from the customer indicating the nature, reason and appropriate details of the foreign transactions sufficient to determine the legitimacy of such transactions.

12.0 Enhanced Customer Due Diligence Measures

Enhanced due diligence measures shall be applied to persons and entities that present a higher risk to Centum. This can broadly be addressed with the following measures:

a) Obtain further information to establish the customer's identity.
b) Apply extra measures to check documents supplied by a credit of financial institution.
c) Obtain senior management approval for the new business relationship or transaction.
d) Establish the person's/entity's source of funds.
e) Carry out ongoing monitoring of the business relationship.

13.0 Centum Policy on Sanctioned Countries

Centum's policy is not to open investment accounts for persons / corporations belonging to countries where comprehensive sanctions are in place. Where such investment accounts are already in Centum's books the same shall be reported to the Regulators for further guidance.

13.1 Country Sanctions

Centum shall not establish a business relationship with persons / corporations where there are U.S. Government sanctions programs or where Centum has a view that a higher AML risk may be posed by allowing Centum's products and services to knowingly or unknowingly be used by such persons. Centum shall thus not allow any transactions touching on the countries listed below:

a) Burma (Myanmar) (Country Sanction)
b) Cuba (Country Sanction)
c) Iran (Country Sanction)
d) Syria (Country Sanction)
e) Sudan (***The sanctions do not apply to South Sudan***)
f) North Korea

13.2 List Based Sanctions

It is important to note that in non-comprehensive programs, there are no broad prohibitions on dealings with countries, but only against specific named individuals and entities. The names are incorporated into OFAC's list of Specially Designated Nationals and Blocked Persons ("SDN list") which includes over 6,000 names of companies and individuals who are connected with the sanctions targets. ***All investment accounts MUST be checked against the UN & SDN lists before they come into the Centum's books.*** Further, all remittances coming into or going out of Centum must be screened before the transaction is processed through the system. A number of the named individuals and entities are known to move from country to country and may end up in locations where they would be least expected. Other non-comprehensive programs apply to the following countries and enhanced due diligence ***MUST*** be undertaken before investment account opening:

a) Belarus
b) Balkans
c) Cote d'Ivoire,
d) Democratic Republic of the Congo,
e) Iraq,
f) Liberia (Former Regime of Charles Taylor),
g) Lebanon,
h) Libya
i) Somali
j) Yemen
k) Zimbabwe

It is the responsibility of the Risk Department to ensure that Centum is kept updated on any changes in this area.

14.0 Centum's Policy on Publicly Exposed Persons (PEPs)

A Publicly Exposed Person means any person who has been entrusted with a prominent public function in (i) Kenya and (ii) a foreign country, and includes:

a) Members of the Cabinet;
b) Senators;
c) Governors;
d) Senior executives of a state owned corporation;
e) An important political party official;
f) Senior military officials and other members of the disciplined forces;
g) Members of the Judiciary;
h) Senior State Officers,
i) Persons who have been entrusted with a prominent function by an international organization who serve as members of senior management i.e. directors, deputy directors or board members.
j) Senior Public Offices; and
k) Any immediate family member or close business associate of a person referred to under the categories a) to h).

Where a customer has been found to be a PEP, Centum shall undertake the following measures, in addition to placing them under medium risk;

a) Obtain approval from senior management to transact/establish the relationship with that person.
b) Take adequate measures to establish the source of wealth and the source of funds which are involved in the proposed business relationship of transaction.
c) Obtain information on immediate family members or close associates of the PEP who may be having transaction authority over the investment account;
d) Determine the terms of the investment account and the expected volume and nature of investment account activity; and
e) Review public sources of information for example the internet, company registries.
f) Once the investment account has been established, conduct enhanced on-going monitoring of the relationship.

In the event that a customer subsequently becomes a Politically Exposed Person after having initially established a relationship with Centum, Centum shall carry out steps a) to c) above immediately it is made aware that a customer is a Politically Exposed Person.

Ascertaining whether a customer has a close association with a senior political figure can be difficult, although focusing on those relationships that are "widely and publicly known" provides a reasonable limitation on expectations to identify close associates as PEPs. A customer may be classified as PEP:

- Where Centum has actual knowledge of a close association, even if such association is not otherwise widely or publicly known.
- By ascertaining the same through CDD i.e. Know your customer procedure

PEPs and related individuals pose unique reputation and other risks.

a) Not all PEPs present the same level of risk. The risk will vary depending on factors such as

geographic locations involved and the individual's position or authority.

b) Financial institutions that conduct business with dishonest PEPs and related individuals face substantial reputation risk, additional regulatory scrutiny, and possible supervisory action. All members of staff are therefore expected to follow reasonable steps to ascertain the status of an individual so as to establish which PEPs may be lower risk and those that may be higher risk for corruption or money laundering.

c) In addition to completing the investment account opening procedures, additional enquiries must be made as to the reputation of the PEP or related individual and should include:

- Consultation with the senior business managers;
- Review of generally available public information (to assess any reputation risk posed by associating with the PEP and related individual) such as news articles from reputable sources.

The interviewer must keep in mind that identification of a customer's status as PEP should not automatically result in a high-risk determination; it is only one factor Centum should consider in assessing the risk of a relationship at the time of investment account opening.

- Once identified as PEP, Centum must conduct a risk-based scrutiny of the transactions and investment accounts held by these individuals.
- Ascertain that the intent is to genuinely utilize Centum's various investment services and products and ***NOT*** to carry out fraudulent transactions including Money Laundering.

d) Investment accounts that are PEP must be indicated as "PEP" when maintaining the investment account opening details within the field provided. Such investment accounts shall be closely monitored by the Subsidiary Director and Risk & Compliance Department.

NOTE: It is Centum's policy that investment accounts for customers rated "high risk" shall be declined at the investment account opening stage. For existing relationships, where the investment account profile changes to "high risk" a decision to terminate the relationship shall be taken immediately.

15.0 Reliance on 3rd Parties

Centum may rely on third parties to perform elements of CDD measures provided that they meet the criteria set out below:

a) The term third parties means other financial institutions or designated non-financial businesses or persons (DNFBPs) that are supervised or monitored by competent authorities.
b) It should be noted that where reliance on third parties to perform elements of CDD measures is permitted, the ultimate responsibility for CDD measures remains with the institution that is relying on the third party.
c) Centum shall immediately obtain the necessary information concerning the relevant elements of CDD measures set out.
d) Centum shall take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to the CDD requirements will be made available from the third party upon request without delay.
e) Centum shall ensure that the 3rd party is regulated, supervised or monitored by a competent

authority and has measures in place for compliance with CDD and record-keeping requirements in line with international best practice.

f) Where Centum relies on a 3rd party that is based out of Kenya, Centum shall assess the AML/CFT risks that the country poses and the adequacy of CDD measures adopted by financial institutions in that country.

16.0 New Products / Technology

a) Centum shall conduct a money laundering and terrorism financing risk assessment so as to assess money laundering and terrorism risks in relations to:
   - New products and new business practices, including new delivery mechanisms; and
   - New or developing technologies for both new and pre-existing products
b) Centum shall ensure that a money laundering and terrorism financing risk assessment is conducted **prior** to the introduction of a new product, new business practice or new technology for both new and pre-existing products.

17.0 Money Value Transfer Services

Centum shall ensure that the providers of money value transfer services are:

a) Licensed or registered by the relevant authorities;
b) Subject to effective systems for monitoring and ensuring compliance with AML/CFT measures;
c) Have AML & CFT programmes in place; and
d) Regularly monitor the AML & CFT programmes for compliance.

18.0 On-Going Monitoring of Transactions

a) On-going monitoring of investment account activity and transactions should be conducted on a risk-sensitive basis.
b) Centum can only effectively control and reduce risk if it has an understanding of normal and reasonable activity of their customers. This shall enable Centum to have the means of identifying transactions which fall outside the regular pattern of an investment accounts activity.
c) Centum shall establish limits for a particular class or category of investment accounts. Particular attention should be paid to transactions that exceed these limits.

18.1 Recognizing and Reporting of Suspicious Transactions

Where Centum becomes aware of suspicious activities or transactions which indicate possible money laundering or terrorism financing, the institution shall ensure that it is reported to the Financial Reporting Centre (FRC) immediately and in any event within seven days of the date of the transaction or occurrence of the activity that is considered suspicious.

It is the duty of every member of staff to:

a) Report to the Senior Risk Officer any suspicious transactions or activity including where there are reasonable grounds to know or suspect. A guide to what could be construed as a Suspicious Transaction can be obtained under Annexure II and III.
b) A review shall be undertaken by the Senior Risk Officer to establish whether there is need for further investigation, or whether there is additional information that removes the suspicion.
c) The key to recognizing suspicions is based on having enough knowledge about a customer's normal expected activity to be able to recognize the abnormal /unusual, and from the abnormal what might be suspicious.
d) The criteria below shall be used to guide staff in identifying suspicious transactions:

I. Suspicious transactions will often be:
   - Any transaction or instruction that is not logical from an economic, financial or banking point or view. Refer to Annexure II and III;
   - Any transaction where the amount, duration or other specific feature is inconsistent with the customer's professional or business activities, or expected investment account activity i.e. out of pattern transactions that cannot be supported.
   - Customers queried more than once by a correspondent financial institution.

II. A query to the remitting institution to confirm KYC and relationship between the parties followed by an immediate recall of the funds without supporting the KYC query initiated by Centum.

III. Customers splitting transactions and failure to avail economic justification for the split transactions.

19.0 Reporting of Suspicious Transactions

All employees are responsible for remaining vigilant to the possibility of ML/TF through use of Centum's products and services.

a) In the case of out-of-pattern transactions, where the Business-line Head is suspicious as to the nature of transactions, they shall immediately bring the investment account to the attention of the Senior Risk Officer.
b) Before escalation to the AML Compliance Unit, the Branch Manager must first interview the customer to understand the transaction and obtain the relevant supporting documentation to support the transaction.
c) The AML Compliance Unit shall undertake an independent review of the investment account to establish whether there is cause for suspicion.
d) Suspicious activities shall be reported to the CEO, Senior Risk Officer, and respective Business Heads for further review and input before a decision to report to the FRC is reached.
e) Where the AML Compliance Unit closes a case escalated by Business-line Head it shall be reported to the ORCO for information and record.
f) If a decision is taken that the matter warrants reporting to the regulatory authority, the Senior Risk Officer shall report the same to the FRC.

19.1 Nature of the Information to be Disclosed

Sufficient information should be disclosed which indicates the nature of and reason for the suspicion.

Where Centum has additional, supporting documentation, that should also be made available.

19.2 Termination of a Business Relationship Following a Disclosure

If, following a disclosure, Centum, exercising its commercial judgment wishes to terminate the relationship with the customer, it is recommended that before taking this step, Centum should liaise with the FRC to ensure that the termination does not in any way "tip-off" the customer or prejudice possible investigation.

19.3 The Suspicious Transaction Report

The Suspicious Transaction Report shall provide sufficient details, regarding the activities or transactions so that authorities can properly investigate and, if warranted, take appropriate action.

20.0 Failure to Report Suspicious Transaction

Centum must note that failure to report suspicious transactions may invite remedial action. Centum is required to be vigilant to ensure it is not used as a conduit for Money Laundering as this will expose Centum to both penalties and reputation risk. To mitigate the risk, Centum shall strictly adhere to KYC procedures, limit transactions with non-investment investment account holders, require supporting documents for transactions over US$.10,000 and be able to identify the high risk investment accounts e.g. PEP, Non-Resident Investment accounts and Forex Bureaus.

21.0 Tipping Off

Where Centum obtains or becomes aware of information which is suspicious or indicates possible money laundering activities, it shall not disclose such information to the customer but shall, report it to the FRC as required by the Prudential Guideline.

22.0 Confidentiality

The queries and inquiries undertaken on suspicious transactions shall in no case be disclosed to the customer. While interviewing the customer, due care must be exercised so that the customers are not informed about the inquiry.

All staff should contact the AML compliance department for any clarification or advice.

It is vital that no mention of the suspicion be made to the customer or anyone outside Centum as it could result in a tipping off offence.

23.0 Staff Awareness and Training

It is a Policy of Centum:

a) To make all management and staff aware of what is expected of them to prevent ML/TF and to advise them of the consequences for them and for Centum if they fall short of that expectation.
b) To provide comprehensive training through learning and development on AML/CDD/CFT to all staff members at least annually.
c) A record of all the members of staff that have been trained shall be availed to the Human Resources Department for their record. AML training shall form part of the annual Training Plan rolled out by the Human Resources Department.
d) AML training shall form part of the Staff Induction Program.
e) That Management and staff are required to sign an undertaking confirming that they have read and understood Centum's AML/CDD/CFT policy and relevant procedures. Changes made on set frequencies or on ad hoc basis to this policy should also be communicated to the staff on a timely basis.

24.0 Record Keeping

It is a Policy of Centum:

a) To retain identification transaction documentation for the minimum period as required by applicable Laws and regulations.
- Centum must ensure that they keep all records obtained through CDD measures such as copies or records of official documents like passports, identification cards or similar documents, investment account files and business correspondence including the results of any analysis undertaken such as inquiries to establish the background and purpose of complex, unusual, large transactions for a period of at least seven years.
- Where the transaction involves a negotiable instrument other than currency, the name of the drawer of the instrument, the name of the institution on which it was drawn, the name of the payee (if any), the amount and date of the instrument, the number (if any) of the instrument and details of any endorsements appearing on the instrument should be retained.

b) To retain records of all reports made by staff to Compliance and all suspicious activity reports made by the Compliance Department to regulators for an indefinite period unless advised by the Regulator otherwise.
c) To be in a position to retrieve, in a timely fashion, records that are required by law enforcement agencies as part of their investigation.
d) To keep records of AML/CDD/CFT training provided to the employees, nature of the training and the names of staff who received such training.
e) To ensure that customer files are updated on a defined basis or when there are major changes – based o the size, complexity &/or risk posed by the relationship. Customer files should also be updated when the customer migrates from one product / investment account class to another.
f) Access to customer files must be on restricted access and investment accountability so as to ensure that nobody tampers with them.

ANNEXURE I: EMPLOYEE CONFIRMATION

EMPLOYEE CONFIRMATION THAT THEY HAVE READ AND UNDERSTOOD CENTUM'S AML/CDD/CFT POLICY AND PROCEDURES

I have read, understand, and agree to comply with the foregoing policies and procedures governing AML/CDD/CFT. I understand that Centum's products / services can be used for AML/TF and undertake to be vigilant and to report any suspicions to the Risk & Compliance Department. I understand that violations of this guideline may subject me to disciplinary action, including termination from employment, legal action and criminal liability where I intentionally fail to comply, hinder an investigation or tip off a customer whose investment account is under investigation. Furthermore, I understand that this policy can be amended at any time and confirm that I shall ensure compliance at all times.

EMPLOYEE NAME:

TITLE:

SIGNATURE:

DATE:

RECEIVED BY RISK & COMPLIANCE DEPARTMENT

NAME:

TITLE:

SIGNATURE:

DATE:

ANNEXURE II: MONEY LAUNDERING SOURCES

Money laundering may not just involve wealth related to Drug Trafficking / Terrorism financing. List of crimes identified by Financial Action Task Force (FATF) as generators of criminal wealth also include:

1) Illegal arms sales
2) Gun running
3) Organized crime including drug trafficking, prostitution and trafficking in human cargo
4) Counterfeiting (including making of imitation and copies of original products / goods)
5) Embezzlement
6) Smuggling (including making of imitation and copies of original products / goods)
7) Fraud, especially computer-supported fraud
8) Benefiting from insider trading
9) Bribery and kickbacks
10) Tax evasion
11) Under and over-invoicing of trade transactions
12) Bogus trade transactions to launder money through round-tripping
13) Facilitating illegal immigration.
14) Foreign official corruption
15) Securities, wire and mail frauds
16) Illegal gambling
17) Racketeering
18) Arson

"PROCEEDS OF CRIME" means any property or economic advantage derived or realized directly or indirectly, as a result of or in connection with an offence irrespective of the identity of the offender and irrespective of whether committed before or after the passing of the Proceeds of Crime and Money Laundering (Prevention) Act and includes, on a proportional basis, property into which any property derived or realized directly from the offence was later successfully converted, transformed or intermingled, as well as income, capital or other economic gains derived or realized from such property at any time since the offence.

NEED TO COMBAT MONEY LAUNDERING (ML) AND TERRORIST FINANCING (TF)

The prevention of ML and TF from the point of view of Centum arises due to the severe nature of consequences of ML and TF:

a) Unexplained changes in supply and demand for money.
b) Volatility of capital flows and exchange rates due to un-anticipated cross border asset transfers.
c) Contamination of legal financial transactions.
d) Systemic risk.
e) Unlawful enrichment by perpetrator of crime.
f) Dampening effect on foreign direct investment.
g) Weakening of social, collective ethical standards.
h) Drug trafficking, human trafficking.
i) Political corruption.
j) Terrorism crimes cause a great deal of human misery.
k) Prudential risks to Centum's soundness arising from these developments.

ANNEXURE III: SUSPICIOUS TRANSACTIONS

The following types of activities or transactions may indicate possible money laundering activities (list is not exhaustive):

Any transaction conducted or attempted by, at, or through a business which one suspects or has reason to suspect:

- Involves funds from illegal activities
- Hides or disguises funds from illegal activities
- Is designed to evade money laundering record or reporting requirements
- Has no business or apparent lawful purpose
- Is not the sort in which the particular customer would normally be expected to engage in
- Actual knowledge
- Wilful blindness or deliberate indifference & conscious avoidance
- Failing to assess adequately the facts and information that are either presented or available and that would put an honest reasonable person on enquiry.

The following types of activities or transactions may indicate possible money laundering activities (list is not exhaustive):

TRANSACTIONS THAT DO NOT MAKE ECONOMIC SENSE

- Transactions in which assets are withdrawn immediately after being deposited, unless the customer's business activities furnish a plausible reason for immediate withdrawal.
- Transactions that cannot be reconciled with the usual activities of the customer, for example, the use of letters of credit and other methods of trade finance to move money between countries where such trade is not consistent with the customer's usual business.
- Transactions which, without plausible reason, result in intensive use of what was previously a relatively inactive investment account, such as a customer's investment account which shows virtually no normal personal or business related activities but is used to receive or disburse unusually large sums which have no obvious purpose or relationship to the customer and/or business.
- Provision of bank guarantees or indemnities as collateral for loans between third parties that are not in conformity with market conditions.
- Back-to-back loans without any identifiable and legally admissible purpose.
- Activity in an investment account that is inconsistent with the customer's business profile in terms of the declared investment account turnover, expected business sources or purpose for which funds are to be utilized.

TRANSACTIONS INVOLVING LARGE AMOUNTS OF CASH

- Large cash withdrawals from a previously dormant/inactive investment account, or from an investment account that has just received an unexpected large credit from abroad.
- The deposit of unusually large amounts of cash by a customer to cover requests for banker's cheques, money transfers or other negotiable and readily available marketable money instrument.

INVESTMENT RELATED INVESTMENT ACCOUNTS

- Purchasing of securities to be held by Centum in safe custody where this does not appear appropriate, given the customer's apparent standing.
- Requests by customers for investment management services where the source of funds is unclear or not consistent with the customer's apparent standing.
- Larger or unusual settlements of securities transactions in cash form.
- Buying and selling of a security with no discernible purpose or in circumstances which appear unusual.

TRANSACTIONS INVOLVING UNIDENTIFIED PARTIES

- Provision of collateral by way of pledge or guarantee without any discernable plausible reason by a third parties unknown to Centum and who have no identifiable close relationship with the customer.
- Transfer of money to another financial institution without indication of the beneficiary.
- Payment orders with inaccurate information concerning the person placing the orders.
- Holding in trust of shares in an unlisted company whose activities cannot be ascertained by Centum.

OTHER RED FLAGS ARISING FROM CORRESPONDENT FINANCIAL INSTITUTION QUERIES

Receiving more than two queries on a customer that seeks to understand the type of business used to generate the funds; relationship between the parties and Centum comfort with the transactions

- A request to a correspondent financial institution for KYC details which results to the correspondent financial institution recalling the funds without confirmation of the details needed to support the KYC.

NOTE:

1. Where remittances are continuously being received from abroad, the AML Compliance team shall query with the correspondent financial institution the source of the funds which are being used for investment locally as well as the relationship and comfort of the correspondent institution to ensure that the KYC on record is fully understood.
2. Where a review establishes that at least 5 out of the parameters highlighted above have been met, it shall call for further review by the Senior Risk Officer, Company Secretary and Corporate Director, Director Finance & Operations, CEO and concerned Business Head with a view to establishing a case to file a STR.

Know Your Client Checklist.

Individuals

- ☐ Original and copy of National ID/Passport of the applicant
- ☐ Copy of PIN Certificate
- ☐ Bank statements for the last 6 Months
- ☐ Two (2) Passport size photos
- ☐ Letter of Introduction
- ☐ Utility Bill
- ☐ Signature Verification

Body Corporate

- ☐ Evidence of registration or incorporation
- ☐ The Act establishing the body corporate
- ☐ A letter from the accounting officer
- ☐ A corporate resolution authorising a person to act on behalf of the body corporate
- ☐ A copy of the latest annual return or financials

In addition to the above, the entity entering into the engagement with the client should avail the following information:

- Statement of nature and source of client's funds
- In the case of a body corporate:
  - Company type
  - Nature of business
  - Physical address
  - Shareholder information that includes the following
    - Number and full names of directors/partners
    - Number and names in full of shareholders

Note that this is in no way a comprehensive list of the information that is required from the entity. This list is subject to changes from time to time. It is the mandate of the entity entering into the engagement to develop their individual investor application form.