FINANCIAL INTELLIGENCE CENTRE
REPUBLIC OF NAMIBIA
P.O.BOX 2882, Windhoek
Tel: **+ 264 61 2835100, Fax +264 61 2835259**
Web address: www.fic.na E-mail address:
leonie.dunn@fic.na

FINANCIAL INTELLIGENCE CENTRE

GUIDANCE NOTE NO.4 OF 2009 ON

THE IMPLEMENTATION OF A COMPLIANCE REGIME

JULY 2009

.

TABLE OF CONTENTS

Description Page

1. Introduction 3
   1.1 General 3
   1.2 Commencement 4
   1.3 Definitions 4
   1.4 Application 4

2. The Financial Intelligence Centre (FIC) 4
   2.1 Functions of the FIC 4

3. Money Laundering 5
   3.1 Criminalization of Money Laundering 5
   3.2 Process of Money Laundering 6

4. Persons or Entities who must implement a Compliance Regime
   4.1 Who must implement a Compliance Regime 7
   4.2 Accountable Institutions 7

5. What is a Compliance Regime 8

6. Adoption, Development and Implementation of a Customer Acceptance Policy 10

7. Appointment of a Compliance Officer 10

8. Internal Rules for Compliance 11

9. Risk-Based Approach 12
   9.1 What is a risk-based approach 13
   9.2 Risk assessment 13
      9.2.1 Products, services and delivery channels 14
      9.2.2 Geographic locations 15
      9.2.3 Other relevant factors 15

9.2.4 Clients and business relationships 15
9.3 Risk Mitigation 17
9.3.1 Measures to mitigate risks 17

9.4 Keeping client identification and beneficial ownership information up to date 19
9.5 Ongoing monitoring 20

9.6 High risk situations for certain sectors 21
9.6.1 Financial entities 21
9.6.2 Financial entities and securities dealers 21

10. Ongoing Compliance Training 22

11. Review 23

12. The FIC'S Approach to Compliance Monitoring 25

13. Penalties for Non-Compliance 26

14. Comments 26

15. How to Contact the FIC 26

Appendix 1:
Products, Services, Delivery Channels and Geographic Locations 27

Appendix 2:
Client and Business Relationships 30

Appendix 3:
Risk Level Assessment Matrix 33

Appendix 4: Schedule 1 of the Financial Intelligence Act, 2007 34

1. INTRODUCTION

This Guidance Note is intended for all accountable institutions listed in Schedule I of the Financial Intelligence Act 2007 (Act No. 3 of 2007) (the Act).

1.1 General

The Act empowers the FIC, to provide guidance to accountable institutions regarding obligations set forth in the Act. This Guidance Note provides guidance that accountable institutions may apply in order to establish a compliance regime, called for primarily in section 25 of the Act. Accordingly, this Guidance Note is primarily directed at accountable institutions (AIs) as listed in Schedule I of the Act, but also can be used by supervisory bodies (SBs) as listed in Schedule II of the Act in their supervisory capacities over accountable institutions..

This Guidance Note is not legal advice and is intended to explain, but not to replace, the language of, the Act and the regulations issued under the Act. Your compliance internal rules may cover situations other than the ones described in this Guidance Note for purposes other than your requirements under the Act.

1.2 Commencement

This guidance note shall come into effect on date of publication in the Government Gazette.

1.3 Definitions

"ACT"	refers to the Financial Intelligence Act, 2007 (Act No 3 of 2007);
"FIC"	means the Financial Intelligence Centre;
"POCA"	refers to the Prevention of Organized Crime Act, 2004 (Act No.29 of 2004), as amended;
"REGULATIONS"	refer to the regulations made under the provisions of section 48 of the Act and published by Government Notice No 74 of 2009 promulgated in Government Gazette No.4253 dated 05 May 2009.

1.4 Application of this Guidance Note

If you are an accountable institution, this Guidance Note has been prepared to help you to implement your compliance regime, to meet your reporting, record keeping and client identification obligations under the (the Act.

Guidance provided by the FIC is the only form of guidance formally recognized in terms of the Act and its complementing regulations. Viewed from this perspective, guidance emanating from industry associations or other organizations, except supervisory bodies, does not necessarily have a bearing on assessing compliance with the obligations imposed by the Act or the interpretation of its provisions.

2. THE FINANCIAL INTELLIGENCE CENTRE

2.1 Functions of the Financial Intelligence Centre

The FIC is Namibia's specialized centre that has been designated under the Act to receive STRs from reporting entities, analyze such reports and disseminate the financial intelligence gathered on suspected money laundering activities to law enforcement agencies, both domestic and international, for further investigation and possible prosecution. The FIC is further empowered to conduct compliance audits on reporting entities in order to ensure compliance with the provisions of the Act. Created in 2006, the FIC is situated in the Bank of Namibia and is an integral part of Namibia's efforts to prevent and combat money laundering.

The FIC was created to detect and deter money laundering by providing critical information to support the investigation or prosecution of money laundering offences.

More specifically, the FIC's function is to:

- receive reports on suspicious transactions (sections 21 and 23(1) of the Act);
- receive reports on cash transactions in excess of prescribed amounts (section 20 of the Act);
- receive reports on electronic transfers of money in excess of prescribed amounts to or from Namibia (section 22 of the Act);
- receive reports on the conveyances of cash in excess of prescribed amounts to or from Namibia (section 24 of the Act);
- receive other information as appropriate (section 5 of the Act);
- analyze and assess the information it receives (section 5 of the Act);
- provide law enforcement agencies with financial intelligence relevant to the investigation or prosecution of money laundering offences and, if such intelligence is relevant to the national security of Namibia, to disclose such intelligence to the Namibia Central Intelligence Service (sections 5 and 34 of the Act);

- ensure compliance by accountable institutions and supervisory bodies with their obligations under the Act and regulations (section 5 of the Act);

3. MONEY LAUNDERING

3.1 Criminalisation of money laundering

The relevant legal statute that criminalizes money laundering is the Prevention of Organized Crime Act, 2004 (Act No. 29 of 2004) (POCA).

Under sections 4, 5, and 6 of POCA, the scope of the crime of money laundering is very broad and entails the following:

(a) disguising the unlawful origin of property (section 4 of POCA);

(b) assisting another person to benefit from proceeds of unlawful activities (section 5 of POCA); and

(c) acquisition, possession or use of proceeds of unlawful activities (section 6 of POCA).

Thus, sections 4, 5, and 6 of POCA describe the various forms of conduct that comprise the crime of money laundering. As such, a money laundering offence may be described as the performing of any act that may result in: (1) concealing the unlawful origin of property (or concealing the fact that such property constitutes the proceeds of crime); (2) assisting another to benefit from unlawful proceeds; and (3) acquiring, possessing, or using unlawful proceeds. Section 4 of POCA includes as criminal conduct, enabling a person to avoid prosecution for money laundering, or diminishing of the proceeds of crime. Under the definition of —proceeds of unlawful activity‖ in POCA, a money laundering offence may also extend to property or proceeds derived from illegal activities that took place outside Namibia.

On the other hand, the Financial Intelligence Act in section 1 defines —money laundering‖ or —money laundering activity‖ as follows:

(a) the act of a person who -

(i) engages, directly or indirectly, in a transaction that involves proceeds of any unlawful activity;

(ii) acquires, possesses or uses or removes from or brings into Namibia proceeds of any unlawful activity; or

(iii) conceals, disguises or impedes the establishment of the true nature, origin, location, movement, disposition, title of, rights with respect to, or ownership of, proceeds of any unlawful activity; where –

(aa) 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

(bb) in respect of the conduct of a person, the person without reasonable excuse fails to take reasonable steps to ascertain whether or not the property is proceeds from any unlawful activity; and

(b) any activity which constitutes an offence as defined in section 4, 5 or 6 of the POCA (as described above).

The Act also contains a number of control measures aimed at facilitating the detection and investigation of money laundering. These control measures, are based on three basic principles of money laundering detection and investigation, namely:

- intermediaries in the financial system must know with whom they are doing business;
- the paper trail of transactions through the financial system must be preserved;
- possible money laundering transactions must be brought to the attention of the FIC.

The control measures introduced by the Act include requirements for institutions to establish the identities of their customers, to keep certain records, to report certain information, and to implement measures that will assist them in complying with the Act. The Act has provided the FIC with the necessary powers to collect, analyze and interpret information that may lead or relate to money laundering and, if necessary, disseminate such information to law enforcement agencies in Namibia.

3.2 Process of money laundering

Money laundering is the process used to disguise the source of money or assets derived from criminal activity. Profit-motivated crimes span a variety of illegal activities, from drug trafficking and smuggling, to fraud, extortion and corruption. Money laundering facilitates corruption and can destabilize the economies of susceptible countries. It also compromises the integrity of legitimate financial systems and institutions, and gives organized crime the funds it needs to conduct further criminal activities. It is a global phenomenon, and the techniques used are numerous and can be very sophisticated. Technological advances in e-commerce, the global diversification of financial markets, and new financial product developments, provide further opportunities to launder illegal profit and obscure the money trail leading back to the underlying crime.

While the techniques for laundering funds vary considerably and are often highly intricate, there are generally three stages in the process:

- Placement which involves placing the proceeds of crime in the financial system;

- Layering which involves converting the proceeds of crime into another form and creating complex layers of financial transactions to disguise the audit trail and the source and ownership of funds (e.g., the buying and selling of stocks, commodities or property); and,
- Integration which involves placing the laundered proceeds back in the economy under a veil of legitimacy.

4. PERSONS OR ENTITIES WHO/WHICH MUST IMPLEMENT A COMPLIANCE REGIME

4.1 Accountable institutions

If you are an accountable institution listed in Schedule I of the Act, you have to implement a compliance regime, as provided under section 25 of the Act (and regulations 13, 21, 22, 23, and 24 which implement section 25 of the Act) Implementation of a compliance regime will assist you to facilitate compliance with your client identification, record-keeping, and reporting requirements under the Act. However, the obligation to implement a compliance regime is being phased in under the current exemptions to the Act as follows:

- All accountable institutions listed under items 1, 3, 5, 6, 12, 13, 14, 15, 16 and 19 of Schedule 1, other than a person registered in terms of section 23 of the Public Accountants'and Auditors' Act, 1951 (Act No. 51 of 1951) who is a member of the Institute of Chartered Accountants of Namibia, are exempt from complying with section 25 of the Act (and regulations 13, 21, 22, 23, and 24 which implement section 25) for six months from the date upon which the Act came into operation, namely, 5 May 2009;

- All accountable institutions listed under items 2 and 4 of Schedule 1 and any person registered in terms of section 23 of the Public Accountants' and Auditors' Act, 1951 (Act No. 51 of 1951), who is a member of the Institute of Chartered Accountants of Namibia, are exempt from complying with section 25 of the Act (and regulations 13, 21, 22, 23, and 24 which implement section 25) for twelve months from the date upon which the Act came into operation, namely, 5 May 2009;

- All accountable institutions listed under items 7, 8, 9, 10, 11, 17 and 20 of Schedule 1 are exempt from complying with section 25 of the Act (and regulations 13, 21, 22, 23, and 24 which implement section 25) for 18 months from the date upon which the Act came into operation, namely, 5 May 2009

In order to assist you in determining in which phase-in category you fall as an accountable institution, we have included Schedule 1 of the Act as Appendix 4 below.

If you are an employee of an accountable institution who (or which) is subject to these requirements, your employer is responsible for the compliance regime. For example, when life insurance agents are employees of a life insurance company, the

life insurance company is responsible for establishing the compliance regime. If you are a life insurance broker or independent agent (i.e., you are not an employee), you are responsible for establishing your own compliance regime.

5. WHAT IS A COMPLIANCE REGIME

The implementation of a compliance regime is a good business practice for anyone subject to the provisions of the Act and its regulations. A well-designed, applied and monitored regime will provide a solid foundation for compliance with the Act. Since all persons and entities do not operate under the same circumstances, your compliance regime will have to be tailored to fit your individual needs. It should reflect the nature, size and complexity of your operations.

If you are a member of an industry association within your sector of activity, you may wish to check with the association to utilize any information developed by the association about anti-money laundering compliance regimes for your industry sector. You may also check with any regulatory body covering your industry sector for any similar information.

As mentioned earlier, your obligations as an accountable institution to establish a compliance regime are set forth in the Act under section 25 (Obligations by Accountable Institutions); and in the regulations implementing section 25, namely, regulations 13 (Customer acceptance policy), 21 (Compliance programmes to be implemented by accountable institutions), 22 (Internal rules concerning reporting of suspicious and unusual transactions), 23 (Internal rules regarding ascertainment and verification of identities), and 24 (Internal rules concerning the keeping of records).

Under this legal framework, your compliance regime must require:

- Adoption, development, and implementation of a customer acceptance policy (section 25(1) of the Act read with the provisions of regulation 13);
- Designation of a compliance officer at management level who will be in charge of the application of the internal programmes and procedures, including proper maintenance of records and reporting of suspicious transactions (section 25(3) of the Act read with the provisions of regulation 21(4));
- Implementation of the compliance regime at branches and subsidiaries of the accountable institution within or outside Namibia (section 25(4) of the Act);
- Development of audit functions to evaluate any policies, procedures and controls developed under section 25 of the Act to test compliance with the measures taken by the accountable institution to comply with the Act and the effectiveness of those measures (section 25(5) of the Act read with the provisions of regulation 21(5)); and
- Internal rules for compliance that include:
    - Confirmation of the responsibility of the management of the institution in respect of compliance with the Act and the internal rules (regulation 21(2)(a));

- Necessary processes and working methods for the proper ascertainment and verification of the identity of persons whom the institution must identify under the Act (section 25(6)(a) of the Act read with the provisions of regulations 21(2)(b) and 23);
- Necessary processes and working methods for the proper record keeping required under the Act (section 25(6)(b) of the Act read with the provisions of regulations 21(2)(d) and 24);
- Necessary processes and working methods to ensure that suspicious transactions are properly reported (section 25(6)(c) of the Act read with the provisions of regulations 21(2)(c) and 22);
- Provisions for training of employees of the institution to recognise and handle suspected money laundering activities (section 25(6)(d) of the Act read with the provisions of regulation 21(3); o Provision that guarantees that Internal rules be available to each employee of an accountable institution (section 25(7) of Act);
- Provisions for disciplinary steps against the relevant staff members for non-compliance with the Act and the internal rules (regulation 21(2)(e)); and
- Process to take into account any guidance notes concerning those duties that may apply to that institution (regulation 21(2)(f)).

6. ADOPTION, DEVELOPMENT, AND IMPLEMENTATION OF A CUSTOMER ACCEPTANCE POLICY

Regulation 13(1) requires that a comprehensive customer acceptance policy (CAP) must be adopted, developed and implemented. The CAP must include clear guidelines and criteria as to the information required and methods to be used in ascertaining and verifying the identity and acceptance of current and prospective clients in accordance with the Act and regulations. The CAP must also include any guidance notes applicable to the accountable institution, setting out international standards to be met in respect of customer due diligence.

Under regulation 13(2), the information required for each prospective client as part of an accountable institution‘s CAP must include:

(a) relevant information pertaining to the client‘s background;
(b) the client‘s country of origin and residence;
(c) any linked accounts that the client or any other party, to the business relationship or single transaction, may have at that institution;
(d) the nature and location of the client‘s business activities, as well as the nature and source of personal income;
(e) the volume or expected volume of transactions in which the client engages or is suspected to engage in; (f) the client‘s business partners; and
(g) any other information that may assist the institution to determine whether the business relationship with the client may be vulnerable to the laundering of the proceeds of corruption or any other crime.

The FIC supports the application of a risk-based approach (explained in detail below in Chapter 9) in the development of a CAP.

7. APPOINTMENT OF A COMPLIANCE OFFICER

The individual you appoint will be responsible for the implementation of your anti-money laundering compliance regime. Your compliance officer should have the

authority and the resources necessary to discharge his or her responsibilities effectively. Section 25 of the Act specifically requires that the compliance officer be appointed at managerial level. Depending on your type of business, your compliance officer should report, on a regular basis, to the board of directors or executive management, or to the owner.

If you are a small business, the appointed officer could be a senior manager or the owner or operator of the business. If you are an individual, you can appoint yourself as compliance officer or you may choose to appoint another individual to help you implement a compliance regime.

As stated above, the compliance officer should be at managerial level and must have direct access to senior management and the board of directors. Further, as a good governance practice, the appointed compliance officer (especially in a large business) should not be directly involved in the receipt, transfer or payment of funds.

For consistency and ongoing attention to the compliance regime, your appointed compliance officer may choose to delegate certain duties to other employees. For example, the officer may delegate an individual in a local office or branch to ensure that compliance procedures are properly implemented at that location. However, where such a delegation is made, the compliance officer retains responsibility for the implementation of the compliance regime.

8. INTERNAL RULES FOR COMPLIANCE

An effective compliance regime includes internal rules and shows your commitment to prevent, detect and address non-compliance. Your compliance program has to include written internal rules to assess the risks related to money laundering in the course of your business activities.

The level of detail of these internal rules depends on your needs and the complexity of your business and will also depend on your risk of exposure to money laundering. For example, the compliance internal rules of a small business may be less detailed and simpler than those of a large bank. However, your internal rules have to be in writing and be kept up to date, whether you are a small business, an individual or a legal entity. Several factors could trigger the need to update, as often as necessary, your internal rules, such as changes in legislation, non-compliance issues, or new services or products.

In addition, if you are a legal entity, your internal rules also have to be approved by a senior officer. A senior officer of an entity includes its director, chief executive officer, chief operating officer, president, secretary, treasurer, controller, chief financial officer, chief accountant, chief auditor or chief actuary, as well as any person who performs any of those functions. It also includes any other officer who reports directly to the entity's board of directors, chief executive officer or chief operating officer.

It is important that your compliance internal rules are communicated, understood and adhered to by all within your business who deal with clients, or any property owned or controlled on behalf of clients. This includes those who work in the areas relating

to client identification, record keeping, and any of the types of transactions that have to be reported to the FIC. They need enough information to process and complete a transaction properly as well to identify clients and keep records as required.

Your employees need to know when an enhanced level of caution is required in dealing with transactions, such as those involving countries or territories that have not yet established adequate anti-money laundering regimes consistent with international standards. See additional information about this in subsection 9.1.2 of Chapter 9 and Appendix 1.

As mentioned earlier, your compliance internal rules must incorporate, at a minimum, the following:

- Confirmation of the responsibility of the management of the institution in respect of compliance with the Act and the internal rules (regulation 21(2)(a));
- Necessary processes and working methods for the proper ascertainment and verification of the identity of persons whom the institution must identify under the Act (section 25(6)(a) of the Act read with the provisions of regulations 21(2)(b) and 23);
- Necessary processes and working methods for the proper record keeping required under the Act (section 25(6)(b) of the Act read with the provisions of regulations 21(2)(d) and 24);
- Necessary processes and working methods to ensure that suspicious transactions are properly reported (section 25(6)(c) of the Act read with the provisions of regulations 21(2)(c) and 22);
- Provisions for training of employees of the institution to recognise and handle suspected money laundering activities (section 25(6)(d) of the Act read with the provisions of regulation 21(3);
- Provision that guarantees that internal rules be available to each employee of an accountable institution (section 25(7) of Act);
- Provisions for disciplinary steps against the relevant staff members for noncompliance with the Act and the internal rules (regulation 21(2)(e)); and
- Process to take into account any guidance notes concerning those duties that may apply to that institution (regulation 21(2)(f)).

It is also recommended that your internal rules include risk assessment and riskmitigation requirements (described immediately below in section 9) applicable to you.

Although directors and senior officers may not be involved in day-to-day compliance, they need to understand the statutory duties placed upon them, their staff and the entity itself.

9. RISK-BASED APPROACH

Your compliance regime has to include an assessment and documentation of risks related to money laundering in a manner that is appropriate to you. This is in addition to your client identification, record keeping and reporting requirements.

A risk-based approach is a process that allows you to identify potential high risks of money laundering and the development of strategies to mitigate the identified risks. Existing obligations, such as your client identification, will be maintained as a minimum baseline requirement. However, when it comes to situations where enhanced due diligence is appropriate, a principle of risk-based approach is to focus your resources where they are most needed to manage risks within your tolerance level. You have to determine what is acceptable for you, taking into account the nature of each product or service, the geographical regions where you do your business and the relationships you have with your clients.

The approach to the management of risk and risk-mitigation requires the leadership and engagement of senior management towards the detection and deterrence of money laundering. The Board, Executive and Senior management is ultimately responsible for making management decisions related to policies, procedures and processes that mitigate and control the risks of money laundering within a business.

9.1 What is a risk-based approach?

In the context of money laundering, a risk-based approach (RBA) is a process that encompasses the following:

- the **risk assessment** of your business activities using certain factors;
- the **risk-mitigation** to implement controls to handle identified risks;
- keeping **client identification** and, if required for your sector, **beneficial ownership information**, up to date; and
- the **ongoing monitoring** of financial transactions that pose higher risks.

These, as well as additional requirements for certain sectors, are explained in further detail in subsections 9.2 to 9.6 herein below.

9.2 Risk assessment

A risk assessment is an analysis of potential threats and vulnerabilities to money laundering to which your business is exposed. The complexity of the assessment depends on the size and risk factors of your business.

While performing your risk assessment, you should refer to Guidance Note 1 of 2009 on Suspicious Transactions for additional, common and industry-specific indicators related to your products and services as well as to occupation, business, financial history and past transaction patterns of your clients. These may help you in completing your risk assessment. Industry associations or regulators may also provide guidance that can be of assistance to you in this regard.

You have to document and consider the following factors in your assessment:

- your products and services and the delivery channels through which you offer the same;
- the geographic locations where you conduct your activities and the geographic locations of your clients;
- other relevant factors related to your business; and
- your clients and the business relationships you have with them.

You may want to perform the risk assessment for your business in two stages:

- Stage 1:
  Business-based risk assessment of your products, services, delivery channels and the geographic location(s) in which your business operates; and

- Stage 2:
  Relationships-based risk assessment of products and services your clients utilize as well as the geographic location(s) in which they operate or do business.

To help you assess products, services, delivery channels and geographic locations that may pose higher risks of money laundering, we have developed a list of questions in a checklist format (see Appendix 1) as well as a risk matrix (see Appendix 3).

Similarly, for clients and ongoing business relationships that may pose higher risks of money laundering, we have developed a list of the most common risk categories in a checklist format (see Appendix 2). See also sub-paragraph 9.1.4 for more information.

Checklists in Appendices 1 and 2 provide examples to facilitate the assessment of the above factors. However, your risk assessment has to be appropriate for your specific business needs which means that it may have to be more detailed than the checklists provided. You can customize the checklists or you can use a different method or another tool. For example, this could take the form of establishing clusters of clients with different risk variables (e.g. products used, geographic location, transaction volumes, business industries engaged in, duration of the relationship, or other factors identified by your business). You could then give the separate clusters a weighting commensurate with the risk of potential money laundering.

Your risk assessment may identify high risk situations for which risk-mitigation controls and monitoring may be required. See sub-paragraph 9.2 and 9.4 for more information.

Risk assessment requires good knowledge of your business operations and sound judgment exercised by your personnel so that the risks for money laundering can be weighed according to each individual factor as well as a combination of them. Your risk assessment is not static and will change over time.

If you are a financial entity or a securities dealer, you have additional requirements related to risk assessment. See sub-paragraph 8.5 for more information.

9.2.1 Products, services and delivery channels

You have to be aware of and recognize products and services or combinations of the same that may pose higher risks of money laundering. Legitimate products and services can be used to mask illegal origins of funds, to move funds to commit crime or to hide the true identity of the actual owner or beneficiary of the product or service.

Products and services that can support the movement and conversion of assets into, through and out of the financial system may pose a high risk. For example, these could include a money laundering related sale of high value goods that resulted in a cheque payable to a bearer which is then deposited into another individual‘s account to make the transaction difficult to trace and detect.

In addition, you may also consider services identified by regulators, governmental authorities or other credible sources as being potentially high risk for money laundering. For example, international correspondent banking services, international private banking services, or services involving banknote and precious metal trading and delivery.

You have to consider, in a manner that is appropriate to you, the channels used to deliver your products or services. In today‘s economy and global market, many delivery channels do not bring the client into direct face-to-face contact with you (for example, internet, telephone or email), and are accessible 24 hours a day, 7 days a week, from almost anywhere. The more remote a client is from you, the more likely you will have to depend on a third party to deliver your products or services. The remoteness of some of these distribution channels can also be used to obscure the true identity of a client or beneficial owners and can therefore pose higher risks. In addition, you should consider new or innovative services or delivery channels that you may use to deliver your products or services.

9.2.2 Geographic locations

You have to consider, in a manner that is appropriate to you, whether geographic locations in which you operate or undertake activities, pose a potentially higher risk for money laundering. Depending on your business and operations, geographic locations can range from your immediate surroundings, whether rural or urban, regional or multiple jurisdictions within other countries.

For example, large entities that operate in a number of domestic jurisdictions may refine the geographic locations factor to differentiate between urban locations having known higher crime rates in comparison to other urban or rural districts. Smaller entities that restrict their activities to a single geographic location or district may not need to make that distinction.

9.2.3 Other relevant factors

You need to consider, in a manner that is appropriate to you, any other factors that are relevant to you, your business or sector. For example, you may offer products or services that can be used to convert funds to a more liquid form, such as electronic wallet, internet payment services or mobile payments. Your business activities may also be more attractive to launder money or fund criminal activity.

Guidance Note 1 of 2009 on Suspicious Transaction Reporting, has more information about money laundering that can help you in your risk assessment. You should also periodically review whether additional factors have become relevant to your situation, like risks arising from innovative or emerging technologies.

9.2.4 Clients and business relationships

The guidance below does not prohibit you from engaging in transactions with potential clients but provides you with information to effectively manage potential money laundering risks.

You have to consider the nature and business of your clients and their relationships with you to determine the level of risk of money laundering. In other words, you have to know your clients to perform a risk assessment. Knowing your clients is not limited to identification or record keeping requirements. It is about understanding your clients, including their activities, transaction patterns and how they operate. Other elements, such as the magnitude of a client's assets or the number of transactions involved, might also be relevant. Although you should obtain this information through your dealings with the client, it does not necessarily mean that you have to ask the client for additional information or identification documents, apart from that which the Act and Regulations require. You should consider clients you do not know as higher risk than those you do know.

Completing a client risk assessment should be appropriate where there is an ongoing relationship. An ongoing relationship is where a client opens an account or undertakes multiple transactions over a time period with you, regardless of whether the transactions are related to each other. Where your dealings with a client are limited to a single transaction, this is **not** considered to be an ongoing relationship. For example, a bureau de change (money services business) would not have to perform a risk assessment for an individual client who conducts a single foreign exchange transaction to buy four hundred ($400) US dollars with Namibian dollars because it is not an ongoing relationship. However, if the transaction seems suspicious, the bureau de change (money services business) has to report it to the FIC as explained in Guidance Note 1 of 2009 on Suspicious Transaction Reporting.

In addition to assessing risk regarding existing clients, for new clients, it is recommended that you perform a risk assessment at the beginning of a client relationship, although a comprehensive risk profile may only become evident once the client has conducted financial transactions with you. However, if you decide to

complete a risk rating of new clients, the client identification and information gathering measures at account opening, should be robust enough to provide the information needed to feed into your client risk assessment.

When assessing a client relationship, consider its duration, the client‘s number of accounts (if applicable), the products and services used and the client‘s activities. You may also consider third parties that can be involved in the client‘s relationship for their impact on the client‘s risk if you are required to make third party determination. Furthermore, you also have to consider the beneficial owners of an entity for their impact on risk if you are required to obtain this information. See Guidance Note 2 of 2009 on Customer Identification for more information about third party determinations and beneficial ownership information requirements.

Situations where you facilitate a transaction for which a client is acting on behalf of a third party, and such client does not know anything about the third party, may lead you to consider that client as a higher risk. Similarly, a client acting on behalf of an entity who is not aware of the entity‘s beneficial owners (such as the names of the entity‘s directors or the individuals controlling the entity for example), may lead you to consider that client as a higher risk.

If you know that your client is a politically exposed foreign person (even when you are not required to make the determination or keep related records), you should consider that client as being a higher risk. See the definition of a politically exposed foreign person in Appendix 2.

You should also consider unusual circumstances, cash-intensive businesses and other indicators as potential high risks.

9.3 Risk mitigation

Risk mitigation is about implementing controls to limit the potential money laundering risks you have identified while conducting your risk assessment, to stay within your risk tolerance level. As part of your compliance program, when your risk assessment determines that risk is high for money laundering, you have to develop written riskmitigation strategies (internal rules designed to mitigate high risks) and apply the same for high risks situations.

9.3.1 Measures to mitigate the risks

You have to include risk-mitigation measures in your written internal rules. The following summarizes different types of mitigating measures you could develop and apply through your internal compliance rules.

Effective internal controls

You should consider internal controls such as:

- focusing on your operations (products, services, clients and geographic locations) that are more vulnerable to abuse by money launderers and criminals;

- informing the Board, Executive and Senior management of compliance initiatives, identified compliance deficiencies, corrective action taken, and suspicious transaction reports filed;

- providing for program continuity despite changes in management, employees or structure;

- focusing on meeting all regulatory record keeping and reporting requirements, recommendations for anti-money laundering compliance and provide for timely updates in response to changes in requirements;
- enabling the timely identification of reportable transactions and ensure accurate filing of required reports;

- incorporating anti-money laundering compliance into job descriptions and performance evaluations of appropriate personnel; and

- providing adequate supervision of employees that handle currency transactions, complete reports, monitor for suspicious transactions, or engage in any other activity that forms part of your anti-money laundering program.

Generic measures

These may include the following:

- increase your awareness of higher risk situations within business lines across your entity;

- increase the monitoring of transactions;

- escalate the approval of the establishment of an account or relationship even if you are not otherwise required to do so (see additional requirements for certain sectors in sub-paragraph 9.5);

- increase the levels of ongoing controls and reviews of relationships; and

- review your own internal controls, to ensure that you have:

    - personnel that have clear lines of authority, responsibility and accountability;
    - adequate segregation of duties (for example, an employee opening an account for a client is not authorized to also approve its opening as that authorization is the responsibility of someone else in the organization);
    - proper procedures for authorization (for example, an employee processing a transaction for which the amount exceeds a certain threshold has to follow a procedure to get approval for the transaction by someone else in the organization); and
    - internal reviews to validate the risk assessment processes.

Risk-focused measures

You may consider additional measures such as:

- seeking additional information beyond the minimum requirements under the Act and Regulations, to substantiate the client‘s identity or the beneficial ownership of an entity;

- obtaining additional information about the intended nature of the relationship, including estimates regarding the amount and type of business activity;

- obtaining additional documented information regarding the client‘s source of funds and accumulation of wealth;

- requesting high risk clients to provide additional, documented information regarding controls they have implemented to safeguard their operations from abuse by money launderers;

- getting independent verification of information (i.e. from a credible source other than the client);

- stopping any transaction with a potential client until identification and account opening information has been obtained;

- implementing an appropriate process to approve all relationships identified as high risk as part of the customer acceptance policy required as part of the compliance regime or declining to do business with potential clients because they exceed your risk tolerance level;

- implementing a process to exit from an existing high risk relationship which management sees as exceeding your risk tolerance level;

- analysing money laundering risk vulnerabilities for your new acquisition processes and for product or service development processes.

If you are a financial entity, a securities dealer, a life insurance company, broker or independent agent, or a money services business, you have additional requirements related to risk-mitigation. See sub-paragraph 9.5 for more information.

9.4 Keeping client identification and beneficial ownership information up to date

When your risk assessment determines that risk is high for money laundering, you have to develop and apply internal rules to keep client identification information up to date. If you are a financial entity, a securities dealer, a life insurance company, broker or agent, or a money services business, this also applies for keeping beneficial ownership information up to date.

Client identification information

Client identification information depends on the information you have to obtain and verify from your clients and the records you have to keep. Client identification information that is required to be updated generally includes:

- For an **individual**, the individual‘s name, address (if possible), telephone number and occupation or principal business.
- For a **corporation**, its name and address and the names of the corporation‘s directors.
- For an **entity other than a corporation**, its name, address and principal place of business.

Reasonable measures to keep client identification up to date include asking the client to confirm or update their information. In the case of an individual client, reasonable measures also include confirming or updating the information through the options available to identify individuals who are not physically present. This can include obtaining information verbally to keep client identification information up to date.

In the case of clients that are entities, reasonable measures to keep client identification up to date include consulting a paper or an electronic document to confirm information or obtaining the information verbally from the client.

Although the frequency with which the client identification information is to be kept up to date will vary depending on your business, you should review it at least every one year for high risk situations. When you review client identification information, you should also update the records you keep for that client.

You may want to consider establishing and implementing a timeline to update the identification information of your clients that you do not consider high risk, but such review and update must take place at least every two years.

Beneficial ownership information

If you are a financial entity, a securities dealer, a life insurance company, broker or independent agent, or a money services business, you have to take reasonable measures to obtain beneficial ownership information about entities in certain circumstances.

Beneficial ownership information of an entity means the name, address and occupation of all the individuals that own or control, directly or not, 25% or more of the entity. If the entity is a corporation, beneficial ownership information also includes the name and occupation of all the corporation‘s directors.

Reasonable measures to keep beneficial ownership up to date are the same as the ones explained for client identification information above. For high risk situations, the beneficial ownership should be updated at least once every year. When you review beneficial ownership information, you should also update the records you keep for that client.

9.5 Ongoing monitoring

You have to take reasonable measures to conduct ongoing monitoring of financial transactions that pose high risks of money laundering, to detect suspicious transactions. Reasonable measures may involve manual or automated processes, or a combination of both, depending on your resources and needs. Last mentioned also depend on the size of your business and the risks to which you are exposed. You do not necessarily have to create or purchase an electronic system. You can use your available resources and business processes and build on these.

Your internal rules have to determine what kind of monitoring is done for particular high risk situations, including how to detect suspicious transactions. Your internal rules should also describe when monitoring is done (its frequency), how it is reviewed, and how it will consistently be applied.

You could consider the following measures to monitor high risk situations:

- review transactions based on an approved schedule that involves management sign-off;
- develop reports or perform more frequent reviews of reports that list high risk transactions. Flag activities or changes in activities from your expectations and elevate concerns as necessary;
- set business limits or parameters regarding accounts or transactions that would trigger early warning signals and require mandatory review;
- review transactions more frequently against suspicious transaction indicators relevant to the relationship and escalate the same should additional indicators be detected. See Guidance Note 1 of 2009 on Suspicious Transactions for more information about indicators.

If you are a financial entity or a securities dealer, you have additional requirements related to ongoing monitoring of financial transactions. See sub-paragraph 9.5 for more information.

9.6 High risk situations for certain sectors

In addition to the risk-based approach process described in sub-paragraphs 9.1 to 9.4, certain sectors have further requirements. These are described below, by sector.

9.6.1 Financial entities

Ongoing monitoring for correspondent banking relationships

When you enter into a correspondent banking relationship with a foreign financial institution, you have to take reasonable measures to find out whether the foreign financial institution has anti-money laundering internal rules in place, including procedures for the approval of opening new accounts. In this context, reasonable measures include asking the foreign financial institution for the information about their internal rules. If it does not have such internal rules in place, you have to take reasonable measures to conduct ongoing monitoring of all transactions (as explained in sub-paragraph 9.4) within the correspondent banking relationship to detect suspicious transactions.

You could also consider monitoring transactions that you have flagged as questionable in the context of correspondent banking relationships such as the following:

- large value or large volume transactions that involve numbered monetary instruments (for example travellers‘ cheques, money orders or bank drafts);

- transactions that appear unusual in the context of the business relationship; or
- transactions that appear to be structured to avoid your monitoring system.

In addition, you have to take reasonable measures to find out, based on publicly available information, whether there are any civil or criminal sanctions imposed against the foreign financial institution in respect of anti-money laundering requirements. If there are any sanctions, the correspondent banking relationship is considered a higher risk. In such case, you have to take reasonable measures to conduct ongoing monitoring of all transactions within the correspondent banking relationship to detect suspicious transactions. To do so, consider the measures described above as well as those in sub-paragraph 9.4.

9.6.2 Financial entities and securities dealers

Politically exposed foreign persons determination for existing and new account holders

If you are a financial entity or a securities dealer, your risk assessment must identify high risk situations for money laundering where existing account holders (including credit card accounts opened by financial entities) might be politically exposed foreign persons. This means that your internal rules have to include reasonable measures to determine whether or not an existing account holder that is considered high risk, is a politically exposed foreign person. You also have to take reasonable measures to determine whether or not a new account holder is a politically exposed foreign person. Whether for a new or an existing account, reasonable measures could include the automated review of your individual client base using commercial software or publicly available information about politically exposed foreign persons. You could also ask your clients.

Once you have determined that an account holder is a politically exposed foreign person, you have additional requirements. This include establishing the source of funds and getting senior management approval to keep an account open (whether for a new or an existing account). You also have to conduct enhanced ongoing monitoring of transactions related to the account to detect suspicious transactions.

10. ONGOING COMPLIANCE TRAINING

If you have employees, agents or other individuals authorized to act on your behalf, your compliance regime has to include training. This is to make sure that all those who have contact with clients, who see client transaction activity, who handle cash or funds in any way or who are responsible for implementing or overseeing the compliance regime, understand the reporting, client identification and verification, and record keeping requirements. This includes those at the —front linell as well as the Board, Executive and Senior management.

Your training program has to be in writing and you have to maintain it. This means that the program itself has to be in writing, but the way the training is delivered does not have to be in writing. For example, you could deliver your training program using computer-based software, information sessions, face-to-face meetings, etc. You also have to ensure that your training program is reviewed and adjusted in a timely manner to reflect your needs.
In addition, others who have responsibilities under your compliance regime, such as information technology and other staff responsible for designing and implementing electronic or manual internal controls, should receive training. This could also include the appointed compliance officer and internal auditors.

Standards for the frequency and method of training, such as formal, on-the-job or external, should be addressed. New people should be trained before they begin to deal with clients. All employees should be periodically informed of any changes in anti-money laundering legislation, internal rules, as well as current developments and changes in money laundering schemes particular to their jobs. Those who

change jobs within your organization should be given training as necessary to be upto-date with the policies, procedures and risks of exposure to money laundering that are associated with their new job.

The method of training may vary greatly depending on the size of your business and the complexity of the subject matter. The training program for a small business may be less sophisticated.

When assessing your training needs, consider the following elements:

- **Requirements and related liabilities**

  The training should give those who need it an understanding of the reporting, client identification and record keeping requirements as well as penalties for not meeting those requirements. For more information about this, see the other guidelines regarding each of those requirements applicable to you.

- **Internal rules**

  The training should make your employees, agents, or others who act on your behalf aware of the internal rules for deterring and detecting money laundering that are associated with their jobs. It should also give each one a clear understanding of his or her responsibilities under these internal rules.

  Employees need to understand how their institution, organization or profession is vulnerable to abuse by criminals laundering the proceeds of crime. Training should include examples of how your particular type of organization could be used to launder illicit funds. This should help employees to identify suspicious transactions and should give you some assurance that your services are not being abused for the purposes of money laundering.

  Employees should also be made aware that they cannot disclose the fact that they have made a suspicious transaction report, or disclose the contents of such a report, with the intent to prejudice a criminal investigation, whether it has started or not. They should also understand that no criminal or civil proceedings may be brought against them for making a report in good faith.

- **Background information on money laundering**

  Any training program should include some background information on money laundering so everyone who needs to can understand what money laundering is, why criminals choose to launder money and how the process usually works. For more information about this, visit the FIC website _ and click on FIC.

All businesses should consult, if possible, training material available through their associations. In addition, the FIC makes material available on its website that can provide help with training. However, as an accountable institution described in Schedule I of the Act, you are responsible to have your own training program and to ensure that each component of the program is reviewed and adjusted to meet your needs.

11. REVIEW

Another component of a comprehensive compliance regime is a review of your compliance internal rules to test their effectiveness. The review has to be done every one year for high risk customers and every two years for low risk customers. It has to cover your internal rules, your assessment of risks related to money laundering and your training program to test its effectiveness. The review or your assessment of risks related to money laundering has to cover all the components of the risk-based approach as explained in sub-paragraphs 9.1 to 9.5, including risk assessment, riskmitigation and ongoing monitoring. This will help evaluate the need to modify existing internal rules or to implement new ones. This may also lead you to update your compliance internal rules.

If you are in a sector that is regulated, the need for review of your compliance internal rules could also be triggered by requirements administered by your regulator.

The review is to be conducted by an internal or external auditor, if you have one. The review by an internal or external auditor could include interviews, tests and samplings, such as the following:

- Interviews with those handling transactions and with their supervisors to determine their knowledge of the legislative requirements and your internal rules.

- a review of the criteria and process for identifying and reporting suspicious transactions.

- a sampling of large cash transactions followed by a review of the reporting of such transactions.

- a sampling of international electronic funds transfers (if those are reportable by the reporting person or entity in question) followed by a review of the reporting of such transactions.

- a test of the record keeping system for compliance with the legislation.

- a test of the client identification procedures for compliance with the legislation.

- a review of the risk assessment.

The scope of the review has to be documented. The scope and details of the review will depend on the nature, size and complexity of your operations. The review

process should be well documented and should identify and note weaknesses in internal rules. The results of the review also have to be documented, along with corrective measures and follow-up actions.

Reporting to senior management

If you are an entity, you have to report the following in writing within 30 days of the review, to one of your senior officers:

- the findings of the above review;
- any updates that were made to the internal rules during the review period;
- the status of implementation of the internal rules updates.

Any deficiencies should be identified and reported to senior management or the board of directors. This should also include a request for a response indicating corrective actions and a timeline for implementing such actions.

Self review

If you do not have an internal or external auditor, you can do a ―self-review‖. If feasible, this self-review should be conducted by an individual who is independent of the reporting, record keeping and compliance-monitoring functions. This could be an employee or an outside consultant. The objective of a self-review is similar to the objectives of a review conducted by internal or external auditors. It should address whether internal rules are in place and are being adhered to, and whether procedures and practices comply with legislative and regulatory requirements.

12. THE FIC's APPROACH TO COMPLIANCE MONITORING

The FIC has a responsibility to ensure your compliance with legislative requirements under the Act. To do this, the FIC can examine your compliance regime and records. The FIC may also periodically provide you with feedback about the adequacy, completeness and timeliness of the information you have reported.

The FIC favours a co-operative approach to compliance monitoring. The emphasis will be on working with you to achieve compliance. When compliance issues are identified, the FIC intends to work with you in a constructive manner to find reasonable solutions. If this is not successful, the FIC has the authority to disclose information related to non-compliance cases to the appropriate law enforcement agencies and/or to take civil or administrative action against you.

The FIC‘s compliance program will use risk management strategies to identify those most in need of improving compliance. Efforts will be focused on areas where there is greater risk of non-compliance and in which the failure to comply could have significant impact on the ability to detect and deter money laundering.

Finally, the FIC will work with other regulators nationally and internationally to identify areas of common interest and address the potential for overlap in some areas of its responsibilities. In that context, the FIC continues to explore avenues for cost efficiencies, consistency of approach and information sharing. Regulators will share information with the FIC when statutorily obligated to do so.

13. PENALTIES FOR NON-COMPLIANCE

Failure to comply with legislative requirements under the Act, can lead to criminal charges against you if you are an accountable institution described in Schedule I of the Act. The following are some of the penalties:

- failure to report a suspicious transaction -- conviction of this could lead to a fine not exceeding five hundred thousand Namibian dollars (N$500,000.00) or imprisonment for a period not exceeding 30 years or to both such fine and imprisonment.
- failure to retain records — conviction of this could lead to a fine not exceeding five hundred thousand Namibian dollars (N$500,000.00) or imprisonment period not exceeding 30 years or to both such fine and imprisonment.
- failure to implement a compliance regime — can lead to an administrative enquiry in terms of section 37, read with the provisions of sections 38, 39 and 40 of the Act. In severe cases of non-compliance, the provision of section 23(9) may be invoked, resulting in a supervisory body of an accountable institution revoking the licence to operate business of such accountable institutions, upon instructions of the FIC.

14. COMMENTS

This Guidance Note shall be reviewed from time to time. If you have any comments or suggestions to help improve this Guidance Note, please send your comments to the FIC by using the particulars provided herein below.

15. HOW TO CONTACT THE FIC

All Correspondence and enquiries must be directed to:

The Director
Financial Intelligence Centre
P.O.Box 2882
No.71 Robert Mugabe Avenue
Windhoek
Republic of Namibia

Tel:+ 264 - 61-2835100
Fax: +264 - 61-2835259
Email: leonie.dunn@fic.na or helpdesk@fic.na

Identify whether you provide any of the following products, services or delivery channels	Yes	No	N/A
For all sectors			
Do you offer services that make it difficult to fully identify clients?			
Do you offer electronic funds payment services? Do you offer any of the following: • Electronic cash (for example stored value and payroll cards)? • Funds transfers (domestic and international)? • Automated banking machines (ABMs)?			
For financial entities			

Do you offer any of the following: • International correspondent banking services involving transactions such as commercial payments for non-clients (for example, acting as an intermediary bank) and use of carriers or couriers for international transport of cash, monetary instruments or other documents (pouch activities)? • Services involving banknote and precious metal trading and delivery? • Electronic banking? • Private banking (domestic and international)? • Foreign correspondent accounts? • Trade finance activities (letters of credit)? • Lending activities, particularly loans secured by cash collateral and marketable securities? • Non-deposit account services (for example, non-deposit investment products and insurance)? • Accounts through which you can extend cheque or bank draft writing privileges to the clients of other institutions, often foreign banks (pass through or payable through type accounts)?			
Services involving an immigrant investor program? Non face-to-face transactions, such as Internet services, by mail or by telephone?			

APPENDIX 1

PRODUCTS, SERVICES, DELIVERY CHANNELS AND GEOGRAPHIC LOCATIONS

The following checklist is intended to provide an example of how to assess risk for your products, services, delivery channels and geographic locations. This is only a starting point and you should customize the checklist for your business.

Your risk assessment tool has to be appropriate for your specific business needs which means that it may have to be more detailed than this checklist for larger

accountable institutions, or entities who conduct large volumes of business. If you already use another risk assessment tool, you can continue to use the same or enhance it as necessary.

If you answer *yes* to any of the questions below, you should consider it as higher risk for money laundering. Where appropriate, risk-mitigation steps should be taken. See sub-paragraph 8.2 for more information.

You can also refer to **Guidance Note 1 of 2009*: Suspicious Transaction Reporting*** for additional indicators or consult to the Financial Action Task Force's Web site at http://www.fatf-gafi.org for further guidance on risk-based approach.

Identify whether you deal with clients or provide products or services in the following geographic locations:	Yes	No	N/A
For all sectors			
Is the client located in a known high crime rate area?			

Do you or your clients operate or undertake activities in the following countries: • Any country subject to sanctions, embargoes or similar measures issued by, for example, the United Nations (UN)? In some circumstances, this will include sanctions or measures similar to those issued by bodies such as the UN, but which may not be universally recognized. • Any country identified as a financial secrecy haven or jurisdiction? • Any country identified by the Financial Action Task Force (FATF) as non-cooperative in the fight against money laundering or subject to a FATF statement? You can consult the current noncooperative countries and territories listed on the FATF Web site at http://www.fatf-gafi.org (select the —Current NCCT listll tab). • Any country identified by credible sources: ○ as lacking appropriate money laundering laws and regulations? ○ ○ as having significant levels of corruption, or other criminal activity? Credible sources means information that is produced by well-known bodies that generally are regarded as reputable and that make such information publicly and widely available. Such sources may include, but are not limited to, supra-national or international bodies such as the World Bank, the International Monetary Fund, the Organisation for Economic Cooperation and Development, and Transparency International as well as relevant national government bodies and non-governmental organisations.			

APPENDIX 2:

CLIENT AND BUSINESS RELATIONSHIPS

The following checklist is intended to provide an example of how to assess risk for your client relationships. This is only a starting point and you should customize the checklist for your business. Your risk assessment tool has to be appropriate for your specific business needs which means that it may have to be more detailed than this checklist for larger reporting entities, or entities who conduct large volumes of business. If you already use another risk assessment tool, you can continue to use it or enhance it as necessary.

If you answer *yes* to any of the questions below, you should consider it as higher risk for money laundering. Where appropriate, risk-mitigation steps should be taken. See sub-paragraph 8.2 for more information.

You can also refer to **Guidance Note 1 of 2009: *Suspicious Transaction Reporting*** for additional indicators or consult the Financial Action Task Force's Web site at http://www.fatf-gafi.org for further guidance on risk-based approach.

Identify whether any of the following apply to the client:	Yes	No	N/A
For all sectors			
Is the client a cash-intensive business?			
Does the client‘s business generate large amounts of cash for certain transactions that are not normally cash-intensive?			
Is the client an intermediary or "gatekeeper" such as a professional that holds accounts for clients where the identity of the underlying client is not disclosed to you?			
Does the client use unsupervised intermediaries within the relationship who are not subject to adequate anti-money laundering obligations?			
Does client identification take place other than face-to-face?			
Does the client reside outside Namibia?			
Does the client deal offshore?			
Is the client an unregistered charity or other unregulated —not for profitll organisation (especially one operating on a —cross-borderll basis)?			
Is the client located in a known high crime rate area?			
Has the client been identified to have engaged in activity that is consistent with the indicators for your sector identified in *Guideline 1 : Suspicious Transactions*?			
Does the comparison between your clients with similar profiles and high levels of assets or large transactions seem unreasonable?			
Does the knowledge of local laws, regulations and rules seem excessive for your client?			
Is the client a new client?			
Do your clients use intermediate vehicles (such as corporations, trusts, foundations, partnerships) or other structures that do not seem usual for their business or seem very complex and unnecessary?			
Does the client offer on-line gaming?			
Does the client‘s structure or nature of its business or relationship make it			
difficult to identify the true owners or controllers?			
Is there a significant and unexplained geographic distance between you and the location of the client?			

Is there frequent and unexplained movement of accounts or funds between institutions in various geographic locations or to different institutions?			
Is the client a politically exposed foreign person? A politically exposed foreign person is an individual who holds or has ever held one of the following offices or positions in or on behalf of a foreign country: • a head of state or government; • a member of the executive council of government or member of a legislature; • a deputy minister (or equivalent); • an ambassador or an ambassador‘s attaché or counsellor; • a military general (or higher rank); • a president of a state owned company or bank; • a head of a government agency; • a judge; or • a leader or president of a political party in a legislature. A politically exposed foreign person also includes the following family members of the individual described above: • mother or father; • child; • spouse or common law-partner; • spouse‘s or common-law partner‘s mother or father and • brother, sister, half-brother or half-sister (that is, any other child of the individual‘s mother or father).			
For financial entities			
Is the client a foreign financial institution with which you have a correspondent banking relationship?			
Is the client a correspondent bank that has been subject to sanctions?			

APPENDIX 3

RISK LEVEL ASSESSMENT MATRIX

You may use the following matrix, as appropriate, when assessing the level of money laundering risks of your products, services and clients. The following matrix is inspired from a matrix included in a document on risk-based approach published by the Financial Action Task Force (FATF).

Low	Moderate	High
Stable, known client base	Client base increasing due to branching, merger, or acquisition	A large and growing client base in diverse geographic area
No electronic transaction services or the Web site is informational or nontransactional	You are beginning electronic transaction services and offer limited products and services.	You offer a wide array of electronic transaction services (i.e., account transfers, or accounts opened via the Internet).
There are few or no large currency transactions.	There is a moderate volume of large currency or structured transactions.	There is a significant volume of large currency or structured transactions.
Identified a few high-risk clients and businesses	Identified a moderate number of high-risk clients and businesses	Identified a large number of highrisk clients and businesses
Few international accounts or very low volume of currency activity in the accounts	Moderate level of international accounts with unexplained currency activity	Large number of international accounts with unexplained currency activity
A limited number of fund transfers for clients, non clients, limited third-party transactions, and no foreign funds transfers	A moderate number of fund transfers, a few international fund transfers from personal or business accounts with typically low-risk countries	Frequent funds from personal or business accounts to or from high risk jurisdictions, and financial secrecy havens or jurisdictions.
Your business is located in an area known to have low crime rate.	Your business is located in an area known to have moderate crime rate.	Your business is located in an area known to have high crime rate.
No transactions with high-risk	Minimal transactions with high-risk	Significant volume of transactions
geographic locations	geographic locations	with high-risk geographic locations
Low turnover of key anti-money laundering personnel and frontline personnel (i.e., client service representatives, tellers, or other personnel)	Low turnover of key anti-money laundering personnel, but frontline personnel may have changed	High turnover, especially in key anti-money laundering personnel positions

APPENDIX 4: SCHEDULE 1 OF THE FINANCIAL INTELLIGENCE ACT

SCHEDULE 1

LIST OF ACCOUNTABLE INSTITUTIONS

(Section 1)

1. Bank of Namibia as defined in the Bank of Namibia Act, 1997 (Act No. 15 of 1997) to the extent that the Bank of Namibia exercises its powers and fulfills its duties under the Bank of Namibia Act, 1997 (Act No. 15 of 1997), the Currency and Exchanges Act, 1933 (Act No.9 of 1933), the Prevention of Counterfeiting of Currency Act, 1965 (Act No. 16 of 1965), and the Payment System Management Act, 2003 (Act No. 18 of 2003).

2. A legal practitioner as defined in the Legal Practitioners Act, 1995 (Act No.6 of 1995).

3. A person who carrier on the business of a trust or keeps in safe custody trust property, a board of executors or a trust company, including a trustee: of a family trust, a settlor of an *inter vivos* or institutional trust.[1]

4. An estate agent as defined in the Estate Agents Act, 1976 (Act No. 112 of 1976).

5. A financial instrument trader.[2]

6. A person who carries on "banking business" or who is "receiving funds from the public" as defined in section 1 of the Banking Institutions Act, 1998 (Act No. 2 of 1998). 7. A person, other than a banking institution, who carries on the business of -

   (a) collecting money from other persons into an account or a fund; or

   (b) depositing the money in such an account or fund into a bank account on behalf of the persons from whom that person has collected the money.

8. A person who carries on the business of a casino or gambling institution.

9. A person who carries on the business of a car dealership.

10. A person carries on the business of second hand goods.

11. A person who carries on the business of trading in minerals specified in Schedule 1 of the Minerals (Prospecting and Mining) Act, 1992 (Act No. 33 of 1992, or high value jewelry, antiques or art.

12. A person who carries on the business of dealing in foreign exchange.

13. A person who carries on the business of rendering investment advice or investment brokering services.

14. A person, who issues, sells or redeems travelers' cheques, money orders, or similar payment instruments.

15. The Post Office Savings Bank as defined in section 1 of the Posts and Telecommunications Act, 1992 (Act No. 19 of 1992).

16. A member of a stock exchange licensed under the Stock Exchanges Control Act, 1985 (Act No. 1 of 1985),

17. A totalisator agency board or a person operating a totalisator betting service,

18. An institution or body designated by the Minister in terms of section 2(2) (p) of the Banking Institutions Act, 1998 (Act No. 2 of 1998),

19. A financial institution as defined in section 1 of the Namibia Financial Institutions Supervisory Authority Act, 2001 (Act No. 30 of 2001),

20. A person who conducts or carries on the business of an auctioneer.