REGENCY
assurance

COMPLIANCE PROGRAM MANUAL

Anti-Money Laundering, Counter Financing of Terrorism & Counter Proliferation Financing Compliance

Implementation Date:
01 January 2016

Date of Update:
01 April 2022

This document has been reviewed and approved by the Executive Management of Regency

COMPLIANCE PROGRAM MANUAL

REGENCY assurance

Table of Contents:

Introduction.....Page 3

General Policy Approach.....Page 3

Explanatory Introduction.....Page 3

Purpose of the Manual .....Page 4

Legislation and Regulatory Standards.....Page 4

Definitions .....Page 5

Internal Policies, Procedures and Controls .....Page 7

AML/CFT/CPF Compliance Program.....Page 8

Role of the Compliance Officer.....Page 8

Risk-Based Assessment.....Page 10

Customer Due Diligence Procedures .....Page 12

Enhanced Due Diligence Procedures .....Page 14

Requirements for Certified Documentation .....Page 16

Record Keeping Procedures.....Page 17

Recognition of Suspicious Activities .....Page 17

Reporting of Suspicious Activities.....Page 19

Employee Training .....Page 20

Audit Function .....Page 22

Independent Audit.....Page 22

General Guidelines .....Page 22

Glossary.....Page 23

1.0 INTRODUCTION

Regency endeavours to be professional and accountable in everything that the business does and further strives to discharge its responsibilities in an ethical and lawful manner.

It is Regency´s policy to conduct all its business in an honest and ethical manner. The business will not seek to influence or be influenced by payments of money, or anything of value, corporate hospitality or gifts.

The firm takes a zero-tolerance approach to incidents of money laundering, bribery or corruption and are committed to acting professionally, fairly and with integrity in all its business dealings and relationships, implementing and enforcing effective proportionate processes to counter money laundering, bribery and corruption.

This policy applies to all individuals working or having responsibilities for Regency and all outsourced services providers, including Directors, Senior Managers, Officers, employees (whether permanent, fixed-term or temporary), consultants, contractors, trainees, seconded staff, home workers, casual workers and agency staff, volunteers, interns, agents or any other person associated with Regency.

2.0 REGENCY´S GENERAL POLICY APPROACH

It is the policy of Regency to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the financing of terrorist or criminal activity.

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the unlawful proceeds appear to have derived from a legitimate source or constitute legitimate assets.

Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal the origin or intended use of the funds, which will later be used for criminal purposes.

Regency has a zero-tolerance approach to any criminal activity or at any attempt at using its clients, processes or products to facilitate money laundering, terrorist finance or criminal activity. All incidents of this nature will be reported to the authorities without exception.

3.0 EXPLANATORY INTRODUCTION

All regulated international entities are required to develop a Compliance Program that must be risked-based and designed to reasonably fulfil the requirements and comply with: Anti-money laundering Regulations (AMLR), No.46 of 2011; Anti-Terrorism (Prevention of Terrorist Financing) Regulations (“ATR”) No.47 of 2011 and; Financial Services (Implementation of Industry Standards) Regulations (“FSR”), No. 51 of 2011 and No. 41 of 2020.

The Financial Action Task Force (FATF) classify Insurance Entities as Designated Non-financial Businesses and Professions (DNFBPs) and are listed as regulated entities under the Proceeds of Crime ACT (POCA), Cap 4.28. POCA, the Terrorist Financing Acts and the St. Kitts and Nevis Financial Services (Implementation of Industry Standards) (Amendment) Regulations, 2020 (FSIISR) place specific requirements and obligations on financial institutions with respect to their roles in combating: money laundering, the financing of terrorist activities and proliferation financing. Accordingly, Saint Christopher and Nevis Financial Services Regulatory Commission have provided guidance protocols on how best to comply with the relevant requirements.

In general, POCA, requires regulated entities, including Insurance Managers, to establish and maintain an anti-money laundering compliance program and to ascertain the identity of their clients. Each regulated entity is required to identify, assess and mitigate the risks that can be abused by criminals for money laundering, terrorist financing and proliferation financing. Internationally, the FATF has developed a series of Recommendations that are recognised as the international standard for combating these and other related threats to the integrity of the international financial system.

By regularly assessing their money laundering, terrorist financing and proliferation financing risks, reporting entities can protect and maintain the integrity of their businesses while contributing to the integrity of the financial system of St. Kitts and Nevis as a whole.

DNFBPs are required to take appropriate steps to identify, assess and understand their Money Laundering, Terrorist Financing & Proliferation Financing (ML/TF/PF) risks in relation to their customers, countries or geographical areas, products, services, transactions or delivery channels. Risk can be jurisdictional; product-related; service-related; client-related or personnel-related. Regardless of where these risks arise, Regency must take reasonable measures to mitigate them.

This expectation is predicated upon the availability and accessibility to this manual and upon each of Regency personnel's knowledge of the business, understanding of the applicable laws and regulations and a careful assessment of the vulnerability to money laundering, terrorist financing and proliferation financing.

4.0 PURPOSE OF THE MANUAL

This Manual has been developed and designed to guide personnel of Regency on the policies and procedures to detect and prevent money laundering, terrorist financing and proliferation financing. A risk-based approach to monitoring and avoiding risk will be taken. This Manual outlines various mechanisms which can be used to ensure that suspicious activities and transactions can be identified and reported to the relevant competent authorities. The policies and procedures outlined have been compiled with the intent to protect the business from being used for illegal purposes and reduce the business' exposure to compliance, legal and reputational risks associated with money laundering, terrorist financing and proliferation.

This Manual has been distributed to all personnel of Regency who have contact with clients.

5.0 RELEVANT LAWS AND INTERNATIONAL REGULATORY BODIES AND STANDARDS

The Manual has been developed in accordance with the following Anti-Money Laundering/ Countering the Financing of Terrorism/Combating Proliferation Financing ("AML/CFT/CPF") Laws and Regulations of St. Kitts and Nevis:

- Financial Services Regulatory Commission Act, Cap 21.10
- Anti-Money Laundering Regulations, No. 46 of 2011 (as amended)
- Anti-Terrorism (Prevention of Terrorist Financing) Regulations, No. 47 of 2011 (as amended)
- Financial Services (Implementation of Industry Standards) Regulations, No. 51 of 2011
- St. Christopher and Nevis Financial Services (Implementation of Industry Standards) (Amendment) Regulations, No. 41 of 2020
- Proceeds of Crime Act, Cap 4.28
- Anti-Terrorism Act, Cap 4.02
- Financial Intelligence Unit Act, Cap 21.09
- The Financial Services (Exchange of Information) Regulations, 2002
- Other related acts and regulations that form part of the AML regime of St. Kitts and Nevis.

In addition to the above-mentioned legislation, the international standards and recommendations developed by the following agencies were used to guide the material provided in the Manual specifically but not limited to the FATF 40 recommendations (recognised as the international standards for combating money laundering and the financing of terrorism; and proliferation of weapons of mass destruction):

- Financial Action Task Force (FATF)
- Caribbean Financial Action Task Force (CFATF)

6.0 DEFINITION OF MONEY LAUNDERING, TERRORIST FINANCING & PROLIFERATION FINANCING

What is Money Laundering?

Money laundering involves any attempt(s) to conceal and/or disguise proceeds gained from illegal sources so that these proceeds appear to have originated from a legitimate source. There are three (3) common features associated with this activity:

- To conceal the true ownership and origin of criminal proceeds;
- To maintain control over the criminal proceeds; and
- To change the form of the criminal proceeds.

The following criminal activities may generate proceeds which may be subject to money laundering activities:

- Fraud;
- Prostitution;
- Theft;
- Drug Trafficking;
- Human Trafficking;
- Embezzlement;
- Bribery and Corruption;
- Electronic Crimes;
- Any others relevant to TF/PF.

This list is an example and is not exhaustive of all various criminal activities which may lead to money laundering.

Money Laundering involves three (3) stages:

Placement – involves physically placing the illegally gained funds into the financial system. This may include the following:

- placing cash on deposit at a bank;
- physically moving cash between jurisdictions;
- making loans in cash to businesses which seem to be legitimate or are connected with legitimate businesses, thus also converting cash into debt;
- purchasing high-value goods for personal use or expensive presents to reward existing or potential colleagues;
- purchasing the services of high-value individuals;
- purchasing negotiable assets in one-off transactions; or
- placing cash in the client account of a professional intermediary.

At this stage, money laundering can easily be detected as this is the first point where the illegal funds enter the financial system.

Layering - distancing the proceeds gained from its criminal source through complex layers of financial transactions, designed to disguise the audit trail and the illegal source to create the appearance of legitimacy. These activities may include:

- multiple wire transfers;

• rapid switches of funds between banks and/or jurisdictions;

• use of cash deposits as collateral security in support of legitimate transactions;

• switching cash through a network of legitimate businesses and "shell" companies across several companies across several jurisdictions; or

• re-sale of goods/assets.

Integration - returning the criminal proceeds which have been laundered back to the criminal or into the economy in such a way that they appear legitimate (e.g. funds used to purchase property or luxury vehicles).

Vigilance systems should be established to capture criminal proceeds moving through the three (3) stages of money laundering. The following points of vulnerability have been identified where it would be more susceptible to detect money laundering:

• cross-border transmission of cash;

• entry of cash into the financial system;

• transfers within and from within the financial system;

• acquisition of investments and other assets;

• incorporation of companies; or

• formation of trusts.

What is Terrorist Financing?

Terrorist Financing (TF) involves the use of funds (legally and illegally obtained) to facilitate terrorist activities.

As previously mentioned, funds involved in money laundering are derived from criminal activities. Due to the fact that terrorist financing may involve legitimately gained funds, the detection and tracing of TF funds can be more difficult than funds used in money laundering.

Terrorists often use formal banking and money transfer systems to transmit funds for their activities. In this regard, systems must be developed and implemented to monitor clients and their transactions to ensure suspicious activities/transactions are detected.

What is Proliferation Financing?

The Financial Action Task Force (FATF) 2010 report has defined proliferation financing as: "referring to the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations."

How can Money Laundering, Terrorist Financing and Proliferation Financing be Combated?

Suitable measures, procedures and policies to combat money laundering, terrorist financing and proliferation financing:

• Approved and implemented Anti-Money Laundering, Counter Financing of Terrorism & Counter Proliferation Financing Program;

• Appointment of a Compliance Officer (CO)/Reporting Officer (RO);

• Implement and perform efficient Know Your Customer (KYC)/Customer Due Diligence (CDD) Procedures;

- Implement Know Your Employee (KYE) Procedures;
- Establish Reporting Procedures of Suspicious Activities internally and to the FIU;
- Establish Appropriate Record Keeping Procedures;
- Promote AML/CFT/CPF culture throughout organization.

7.0 INTERNAL POLICIES, PROCEDURES AND CONTROLS

Regency shall develop and maintain an adequate and effective risk-based compliance program to deter persons from making use of its facilities for the purpose of money laundering, terrorist financing and proliferation financing. This compliance program will apply to all personnel within the business who are required to follow the established policies and procedures to ensure that they conduct their duties and the duties of the business in accordance with these guidelines and AML/CFT/CPF Laws and Regulations of St. Kitts and Nevis. In addition, all personnel will undergo a period of training and will be required to certify in writing that they understand the duties and obligations outlined within this Manual and the AML/CFT/CPF Laws and Regulations of St. Kitts and Nevis.

Personnel who fail to conduct their duties in accordance with the duties and obligations outlined within this Manual will be subject to an evaluation and disciplinary action(s) as per Regency policies on these matters.

Compliance Requirements

Regency will:

1. Develop, implement, monitor and maintain an effective risk-based AML/CFT/CPF Compliance Program, in line with the relevant guidelines, laws and regulations of St. Kitts and Nevis, and international standards.
2. Develop and implement policies, procedures, processes and controls designed to prevent and detect potential money laundering and terrorist financing activities. These shall include the following:
   - Risk Assessment;
   - Customer Due Diligence (CDD)/Know Your Customer (KYC) Procedures;
   - Record Retention Policy;
   - Training and Awareness Program(s);
   - Personnel Screening Procedures;
   - Mechanisms for the detection of unusual/suspicious transactions;
   - Monitoring and Reporting Procedures; and
   - Independent Audit.
3. Appoint a competent Compliance Officer (“CO”) and/or Reporting Officer (“RO”) to oversee the AML/CFT/CPF program.
4. Ensure that the established policies, procedures and controls are communicated to all relevant personnel.
5. Establish and implement an ongoing training program to ensure that all personnel are well informed and up-to-date with emerging and new trends and developments relating to money laundering and terrorist financing.
6. Contract the services of a suitably qualified auditor to establish and implement an independent audit test that will review and assess the effectiveness of the AML/CFT/CPF program to ensure appropriate measures are applied to recognize suspicious activity and mitigate the risks associated with money laundering and terrorist financing.

7. Establish and implement an on-going screening procedure to ensure that all personnel are fit and proper to conduct the duties required of the business.

8.0 AML/CFT/CPF COMPLIANCE PROGRAM

Regency's AML/CFT/CPF Compliance Program ('the Program') is developed to meet the regulatory requirements of the Financial Services Regulatory Commission (FSRC) Act and compliance with the AML/CFT/CPF Laws and Regulations of St. Kitts and Nevis. The ultimate objective of the Program is to establish appropriate mechanisms to assist the business operations in detecting and preventing money laundering, terrorist financing and proliferation financing.

The Manual provides a comprehensive overview of the Program and provides three (3) critical components:

1. **Awareness** – Personnel should be aware of the importance of compliance and carry out his/her respective duties to ensure its effective implementation.
2. **Advice** – The CO plays a key role in the implementation of the program. This officer should provide all personnel with guidance regarding their respective duties under the program and the business' operations. The CO should also aid in the promotion of the importance of close collaboration the Executive Management team and personnel to ensure the objective of the program is met; and the level of risk associated with conducting business is determined and appropriately mitigated.
3. **Recognition and Reporting** – The program should clearly outline mechanisms to recognize, analyze/investigate and report suspicious activities.

9.0 ROLE OF THE COMPLIANCE OFFICER (CO)/ REPORTING OFFICER (RO)

The compliance function is now viewed as an integral part of the business process due to changes in regulatory approach and international standards. With compliance now being one of the key measures within the business operations this has led to the evolution of COs. COs now demonstrate the value added to business in terms of risk mitigation, decision making, training, and product design amongst other related matters.

Regency will designate a CO who will be responsible for implementing an effective and efficient compliance program in accordance with the AML/CFT/CPF Laws and Regulations of St. Kitts and Nevis and relevant international standards. The role of the CO is an independent and objective function which oversees the AML/CFT/CPF Compliance Program. This function would therefore require the CO to have an excellent understanding of the business in general; flexibility, be open-minded as well as sensitive to different cultures; and cognizant of the ever-changing regulatory environment. The designated CO should also be an ethical and proactive individual who is vigilant. Additionally, the individual should undertake the necessary steps to enforce the established policies and procedures and review and evaluate the strengths and weaknesses of the compliance program within the business.

The Designated CO should:

- Ensure that the entity's/regulated person's business is conducted in compliance with international and local professional standards and accepted business practices;
- Ensure that the Executive Management and all personnel are aware of the business' AML/CFT/CPF obligations, so that such could be factored into respective duties for the business to be in compliance with the established rules and Laws and Regulations of St. Kitts and Nevis;
- Develop, implement, monitor and revise policies and procedures for the business' AML/

CFT/CPF Compliance Program, in accordance with the AML/CFT/CPF Laws and Regulations of St. Kitts and Nevis; and international standards;

- Ensure that the ML/FT/PF risks associated with conducting business are identified and understood by Management; and compliance systems are implemented within the business operations to mitigate these risks;
- Evaluate, monitor and manage legal, compliance and reputational risks associated with the business to safeguard its operations against vulnerability and manipulation; and develop contingency plans, where necessary;
- Collaborate with all other personnel to ensure that all practices and procedures are in accordance with the business' AML/CFT/CPF Compliance Program and relevant legislation;
- Periodically review the Compliance Program to measure efficiency and effectiveness and to identify potential areas for improvement;
- Monitor and, as necessary, coordinate operational activities of other departments to remain consistent with all established compliance activities; and to identify any trends and weaknesses;
- Develop and implement corrective action plans for the resolution of problematic issues and provide general guidance on how to avoid/deal with similar situations in the future;
- Provide reports on a regular basis as applicable to the Executive Management team to keep them informed of the operation and progress of compliance efforts;
- Ensure that all suspicious activities to be forwarded to the Financial Intelligence Unit (FIU) have been submitted;
- Be the point of contact for the FIU concerning money laundering, terrorist financing and related matters;
- Document, investigate and maintain all suspicious activities/transactions reported internally;
- Develop and manage the Register of Suspicious Activity Reports containing all noted suspicion reported and not reported to the FIU;
- Develop and manage the Register of Enquiries containing all enquiries received from the relevant competent authorities such as the FIU;
- Coordinate with the Executive Management team, as appropriate, to develop an effective training program. This would include on-going training for existing personnel and appropriate introductory training for new personnel;
- Ensure that the issues relating to ethics and compliance are evaluated, monitored, managed and resolved in an appropriate manner;
- Ensure that the monitoring and reporting mechanisms are in place to recognize, investigate and report suspicious activity or any other activities that appear unusual to the normal course of client's business or type of client's transactions.

The roles and responsibilities outlined above are in accordance with Section 12 of the Anti-Money Laundering Regulations, 2011, the Anti-Terrorism (Prevention of Terrorist Financing) Regulations, 2011.

The Designated CO must align the compliance program with the operations of the business in order to improve its overall performance. The relationship between two concepts: risk management and compliance will allow the alignment of the compliance and expressed values and objectives within the business to be incorporated in the overall context of the strategic vision.

The Designated CO should emphasize to all personnel that being fully compliant is essential to any expansion of business. By reducing compliance risk, a business commits itself to a path of even greater compliance and the creation of added value.

Regency may also appoint a RO to work in tandem to the CO or appoint the CO as the RO.

In accordance with the AML/CFT/CPF Regulations, the RO would be responsible for receiving and considering reports regarding suspicion.

10.0 RISK-BASED ASSESSMENT

The Financial Services (Implementation of Industry Standards) Regulations requires Regency to assess the risk of a prospective client prior to entering into a business relationship with the applicant. Risk-based management remains pivotal to Regency. Therefore, a risk-based assessment will be conducted to determine the risk level of each applicant, the required financial services product, and any other relevant factors. Based on the assessment, it will be decided whether or not to accept a business relationship with a prospective client or continue an existing relationship.

In performing said assessment, Regency will ensure that all risk management processes align with the ISO 31000 framework which covers the essential aspects of risk management practices in organisations.

This framework is in line with international standard of risk management, and incorporates necessary elements of the applicable laws of St. Kitts and Nevis. It also includes eight major elements namely: risk identification, risk assessment, risk evaluation, risk reporting, decision, risk treatment, residual risk reporting and monitoring. Elements of this process will be applied throughout the AML/CFT/CPF compliance program at various stages.

The risk assessment process takes into consideration whether the client is new or an existing one. The general steps to be taken would include:

- identifying the customer type;
- the collection of identification documents;
- conducting customer due diligence;
- utilizing investigative software and search engines via the World Wide Web.

More detailed factors for consideration are listed below:

- The products and services offered and the delivery channels through which they are offered;
- The geographic locations where the business activities are conducted and the geographic locations of clients;
- Nature and frequency of the activities;
- The complexity of the account/business relationship;
- Value of the account/business relationship;
- Customer type (e.g. Politically Exposed Person [PEP], Non-bank Financial Institution, Cash Intensive, Virtual Asset Service Providers);
- Whether client/customer is the beneficiary of a life insurance policy;
- Whether client's/customer's account/business relationship is dormant;
- Whether there is a form of delegated authority in place (e.g. power of attorney);
- Company issuing investments;
- Cash Intensive;
- Cash withdrawals/placement activity in or outside the jurisdiction;
- Delivery channels and payment processes;
- The clientele and the business relationship;
- Suspicion or knowledge of money laundering, financing of terrorist activities or other crimes

such as fraud; and

• Any other relevant factors related to the business.

*This list is not exhaustive.

Personnel would also review various sanction lists (e.g. OFAC, United Nations) and websites of the FSRC and FIU for information regarding high risk customers and countries.

Risk Identification/Risk Analysis/Risk Evaluation

The inherent risk which exists for the business when providing designated products/services must be identified. Inherent risk is the risk that an activity would pose if no controls or other mitigating factors were in place. It is intrinsic to the business activity and arises from exposure to and from the uncertainty of potential future events.

Key to the risk assessment process is the analysis of potential threats and vulnerabilities to money laundering, terrorist financing and proliferation financing to which there is risk exposure to Regency. This process takes into consideration the organization's size and likely risk factors. Sound judgment must be exercised so that the money laundering, terrorist financing and proliferation financing risks can be weighed according to each factor as well as a combination of them. The risk analysis, and therefore the risk assessment, is not static and will change over time. Risk management systems will be updated to ensure that the company remains fully compliant.

Regency will evaluate any potential risk whether it may be internal or external and report to the Executive Management Team where necessary in an effort to avoid AML/CFT/CPF.

A risk rating score is then assigned to both the probability that each risk might occur and the corresponding potential impact of that occurrence. A simple scale will be used to classify each risk probability or potential impact as either:

• 1 = Low (L)

• 2 = Medium (M)

• 3 = High (H)

Clients

Regency must identify the risk of doing business with each client based on the factors outlined above. Personnel would review the information submitted by each potential client and determine risk prior to entering into a business relationship. Each applicant will be assigned a risk rating after all factors have been considered. The decision on whether to enter into a business relationship or exit an existing business relationship would be based on the risk rating determined. This rating would also be used to determine the monitoring processes for each client.

If the client receives an overall risk rating of Low or Medium, the application to conduct business may be approved by personnel. However, if the client receives an overall risk rating of High, the application to conduct business should be forwarded to Executive Management/ CO for consideration of the matter and a decision on whether the business of the client would be accepted or continued.

This risk rating would form a part of the customer profile of the approved client. These customer profiles should be documented and be in accordance with the record retention keeping policy of Regency.

Business Operations

Regency would also assess its own vulnerability with respect to money laundering, terrorist financing proliferation financing risks.

The following categories of inherent risk should be considered:

- Market;
- Operational;
- Legal and Regulatory;
- Strategic;
- Reputation;
- Concentration;
- Credit;
- Geographical;
- Nature and diversity and complexity of the business;
- National Risk-Assessment (NRA) of St. Kitts and Nevis; and
- National Risk-Assessment (NRA) of other relevant applicable jurisdictions.

After the identification of the inherent risks which are likely to be encountered while conducting business, these risks are then assessed in terms of a combination of likelihood that these risks will occur, and the impact of the consequence of loss or severity of damage that may result. Resources should be allocated to efficiently and effectively mitigate the identified risks.

General

Management should be able to build expectations based on the type and rigour of risk management and controls that would be required to effectively manage the key risks to reduce them to acceptable levels, thereby developing the entity's/regulated person's risk appetite. The CO will conduct regular assessments to determine whether the mitigating controls and programs identified are indeed functioning as per the policy and processes that have been established to safeguard the integrity and reputation of the business.

The Risk Assessment process of the business will be ongoing. Unforeseen events such as significant reorganizations, mergers, and acquisitions may create opportunities for refreshing the risk assessment. Management must be able to continually deploy resources in the most effective manner, and as such, this requires a current and accurate understanding of the risks.

Risk Monitoring

Regency will continually monitor its risk as it relates to AML/CFT/CPF. This would be undertaken by using various risk monitoring and management techniques. Regency will also seek to analyze international trends and changes in legislation and seek to incorporate such changes as and when it becomes necessary.

The following circumstances will prompt an additional risk assessment:

- Changes in the nature of business;
- Introduction of new business or services;
- Growth through mergers and acquisitions;
- Entry into new markets; and results of the country's NRA.

11.0 VERIFICATION/CUSTOMER DUE DILIGENCE (CDD) PROCEDURES

When entering into a business relationship with prospective clients (individual and/or corporate), Regency will conduct a thorough and objective examination on the personal information and supporting documentation submitted by each client to establish his/her identification. In addition, personnel would review other preliminary information deemed necessary to aid them in determining the risks, if any, associated with the client.

This examination may be multi-dimensional depending on the type of service(s) desired. A combination of various types of due diligence may be required: Commercial Due Diligence, Reputational Due Diligence, Financial Due Diligence, and Legal Due Diligence.

Personnel will ensure that all engagement documentation (e.g. client agreement, application form, etc.) are duly completed and signed before the business relationship is established. The AML/CFT/CPF Laws and Regulations of St. Kitts and Nevis require regulated entities/persons to establish Customer Due Diligence (CDD)/Know Your Customer (KYC) procedures to obtain the origin and background of each customer/client. The designated risk factor shall determine the extent of any CDD or KYC procedures to be followed in respect of each individual client.

The Financial Services (Implementation of Industry Standards) Regulations require regulated entities/persons to consider the usefulness of the following personal information:

- full name(s) used;
- date and place of birth;
- nationality;
- current permanent address, including postal code;
- telephone, e-mail address and fax number (if available);
- occupation and name of employer (if self-employed, the nature of the self-employment); and
- specimen signature.

This information may be collected on the Application Form which each client would be required to complete.

Other supporting documents that may need to be collected along with the completed Application Form to verify the identity of the client include but are not limited to:

- Copies of government-issued photo identification notarized by a notary public. Acceptable forms of government-issued photo identification are current valid passport, national identity card, social security card and driver's licence;
- Documentation to verify the client's physical address;
- Letters of reference: i.e from a Banking institution which has conducted business with the client previously or another from a professional (e.g. lawyer, accountant, etc.); and
- Police/Criminal Affidavit/Certificate/Record.

All documents should be in their original format or notarized true copies.

In the case of a corporate client, the entity/regulated person should obtain the origin and background of the business and an understanding of its corporate structure and its beneficial owners. In addition to the abovementioned information, which would be collected for all beneficial owners and directors, information/documents which should be collected for insurance related companies at the point of entry to business are, as follows:

- Certificate of Registration/Incorporation;
- Certificate of Good Standing (if applicable);
- Statutory Statement (if applicable);
- Memorandum of Association/Articles of Incorporation and Articles of Association/Bylaws;
- Current Register of Members/Directors and Officers (if applicable);
- Certificate of Incumbency (if applicable);
- Trust Agreement;
- Identification of the Control Persons in line with the individual due diligence requirements;

- Copy of the most recently audited financial statements – certified by Regency Personnel if necessary.

The above list is not exhaustive.

Paragraph 85 of the Financial Services (Implementation of Industry Standards) Regulations requires that all copies of documentation collected should be certified, indicating that the relevant personnel have seen the original documentation.

The due diligence process should be an on-going process. The files would be reviewed at stipulated intervals as determined by the risk assessment rating process. (See Section 12.0)

All documentation obtained for each client should be secured appropriately.

The information collected and maintained would be utilized to establish a customer profile for each client.

Specific to Authorized Service Providers

Introduced Business

The Financial Services (Implementation of Industry Standards) Regulations require regulated entities/persons to develop procedures for receiving Introduced Business from Professional Service Clients (PSC). Professional Service Clients are defined as organizations or persons, such as law firms, accountants, banks, trust companies and similar professional organizations who contract the services of a fiduciary on behalf of its clients.

All business conducted by Regency is licensed and regulated in its own right. Therefore, due diligence procedures apply regardless of the origin of the business.

Life Insurance Business

As it relates to life insurance business, as prescribed by regulations, identification and verification of the beneficiary should take place as soon as that beneficiary is identified or designated and, in all cases no later than the time of pay-out. Regency will ensure that said verification and identification is done for all beneficiaries of life insurance policies at latest at the time of pay-out or at the time when the beneficiary intends to exercise their vested rights under the policy.

The beneficiary of a life insurance policy who is a legal person or legal arrangement and who presents a higher risk, will be subject to enhanced due-diligence measures prior to or at the time of pay-out.

12.0 ENHANCED DUE DILIGENCE PROCEDURES

Enhanced Due Diligence is required where a client and/or product/service are considered to be of greater risk. This higher level of due diligence is required to mitigate the higher risk identified during the initial due diligence process of the client. A high-risk situation generally occurs where there is an increased opportunity for money laundering or terrorist financing through the manipulation of the service and product by the client.

In such cases, additional due diligence is necessary to verify the client's identity or source of wealth or perhaps an adverse media publishing. The client would be required to provide additional corroborative information or provide information specific information regarding "Source of Wealth/Funds". The additional checks conducted or supplementary information collected should be relative and proportionate to the level of risk identified. These additional mechanisms should create a better understanding of the client and provide confidence that any possible risk identified has been mitigated or is unlikely to be realized. Further, the Enhanced Due Diligence performed for higher-risk clients is especially critical in understanding their anticipated transactions and implementing a monitoring system that reduces the entity's/ regulated person's reputation, compliance and transaction risks.

The Enhanced Due Diligence procedures to be conducted on high-risk clients whether domicile or international include, but are not limited to:

1. Verifying source of funds for cash and cash equivalents in excess of the threshold or outside of the expected income based on employment/business;
2. Financial Statements;
3. Banking References;
4. Reports/Findings retrieved from credible verification database systems such as World Check; and
5. Conduct enhanced monitoring of business relationships. Politically Exposed Persons (PEPs).

Regency will determine whether a client is considered a PEP through the customer due diligence and risk assessment measures outlined above. Further, the relevant personnel will determine whether the client is a domestic or foreign PEP (See Glossary).

Foreign PEPs are considered to be inherently high risk. In addition to the normal customer due diligence procedures, the following is required for business relationships with foreign PEPs:

- Executive management approval for establishing (or continuing for existing clients) business relationships;
- Establish source of wealth and source of funds; and
- Conduct enhanced monitoring of business relationships. Domestic PEPs also carry some level of risk but would be assessed on a case-by-case basis. Normal customer due diligence would apply to Domestic PEPs. If upon assessment, a Domestic PEP is considered high risk or involved in activities deemed to be high, the procedures outlined above for Foreign PEPs would apply.

Ongoing Due Diligence

Due Diligence (normal and enhanced) should be an ongoing process and the entity would take measures to ensure that client files are current and whether the risk rating of the client has changed. There would be a regular review of the files to ensure that all due diligence is current, and updated information is obtained from the client where necessary.

The risk rating of the client would determine the monitoring interval:

- Low - no more than 24 months;
- Medium - no more than 18 months; and
- High - no more than 12 months.

In cases where the client's activities/transactions are not consistent with his/her profile an investigation would be conducted. The client's risk profile would be adjusted and/or additional investigations would be conducted. If the inconsistency in the client's profile is deemed suspicious, a suspicious activity report will be filed with the FIU.

Personnel are required to conduct ongoing monitoring on all clients to verify if the client's position/profile is consistent or has deviated from the profile previously determined. Clients with transactions/activities that appear to be inconsistent with their profile or business activities may be required to provide additional information necessary to provide an additional level of comfort/assurance.

In addition to the client completing the various assessment forms, if during the monitoring process, personnel note material changes in the nature, volume or size of the client's transactions, the following steps should be taken:

- Updated due diligence should be obtained from the client;
- Question the client to establish any changes in the composition or nature of the business or the purpose of the change in activity;
- Visit the client place of business, if deemed necessary and if possible;
- Establish whether the risk of the client has changed and if measures should be instituted to mitigate the risk associated with this client.

One-Off Transactions

Regency shall conduct the above CDD and KYC measures in relation to every relevant business transaction, including one-off transactions.

13.0 REQUIREMENTS FOR NOTARIZED/CERTIFIED DOCUMENTATION

Where Regency relies on a copy of a document in the establishment of a business relationship or conduct of a transaction with a customer or applicant for business, the copy of the document shall be:

(a) legible; and where necessary

(b) notarized/certified in accordance with the requirements set out in this manual.

A regulated business shall rely on a document as a notarized/certified document where:

(a) the document is notarized/certified by a person who is subject to professional rules of conduct which provide the service provider with a reasonable level of comfort as to the integrity of the certifier;

(b) The person certifying the document indicates that

(i) he or she has seen original documentation verifying the person's identity or residential address;

(ii) the copy of the document being notarized/certified is a complete and accurate copy of that original; and

(iii) in a case where the documentation is to be used to verify the identity of an individual and contains a photograph, the photograph contained in the notarized/certified documentation bears a true likeness to the individual requesting certification;

(c) the certifier has signed and dated the copy of the document, and provided adequate information so that he may be contacted in the event of a query; and

(d) if the certifier is located in a higher risk jurisdiction, or where the service provider has some doubts as to the veracity of the information or documentation provided by the applicant and the service provider has taken steps further to those in paragraph (a) to establish that the certifier is real.

Regency shall satisfy itself that the person certifying the document:

(a) is independent of the individual, or Regulated Entity for which the certification is being provided; and

(b) is subject to professional rules of conduct or statutory AML/CTF/CPF measures.

Where the certification has taken place in a 'high risk country' or Regency doubts the veracity of the information or documentation provided, Regency shall take such steps that it considers necessary to satisfy itself as to the veracity of information or documentation provided.

Regency standard is to accept only notarized documents.

14.0 RECORD KEEPING PROCEDURES

Regency shall maintain all information (electronically) obtained during the course of business for a minimum of five (5) years from the date the business relationship ends.

The following documentation will be maintained:

- All customer due diligence information obtained on all directors and beneficial owners including client's Identification cards, passport ID page, address, telephone, and proof of address;
- Source of Funds/Wealth Information;
- Share Register or other document clearly showing ownership of business previously established;
- Document identifying the Directors of the previously established entity;
- Document containing the findings of a search done on World Check or another credible investigative database;
- All Suspicious Transaction Reports (STRs)/Suspicious Activity Report (SARs) filed with the FIU and the consolidated registers for such reports; and
- All enquiries received from the relevant competent authorities.

15.0 RECOGNITION OF SUSPICIOUS ACTIVITIES AND AML/CFT/CPF MONITORING

Suspicious transactions/activities are transactions/activities for which there are reasonable grounds to suspect that the activities/transactions are related to the commission of a money laundering or terrorist financing offence. Reasonable grounds to suspect suspicious transactions/activities are determined by the circumstances presented. It is important to establish the client's profile outlining his/her normal activities to recognize when an activity/transaction is suspicious. Personnel should be cognizant of the financial flows and activity/transaction patterns of clients to identify unexpected changes in behaviour related to the client's normal activities/transactions (as outlined within the profile).

Special attention must be paid to the following types of activities/transactions:

- Business transactions with individuals, corporate persons and financial institutions in or from other countries which do not or insufficiently comply with the FATF 40 Recommendations;
- Business transactions with individuals, corporate persons and financial institutions in or from other countries which have been deemed to be high risk by recognized international bodies/agencies;
- Business transactions with individuals, corporate persons and financial institutions which appear on sanctions lists such as the OFAC list and UN list;
- A transaction which is complex, unusual or large, whether completed or not;
- Unusual patterns of transactions such as insignificant but periodic transactions which have no apparent or visible economic/lawful purpose;
- Two or more one-off transactions which appear to be linked;
- Changes in the activities or lifestyle of the clients; and
- Adverse or derogatory information discovered during ongoing due diligence or media searches.

Identifying Suspicious Activities/Transactions

Activities/Transactions, whether completed or attempted, may give rise to reasonable grounds to suspect that they are related to money laundering or terrorist financing activities regardless of the sum of money involved.

There is no monetary threshold for making a report on a suspicious transaction. A suspicious transaction may involve several factors that may on their own seem insignificant, but together may raise suspicion that the transaction is related to the commission or attempted commission of a money laundering offence, a terrorist financing offence, or both.

Transactions must be evaluated in terms of what seems appropriate and is within normal practices of the business and knowledge established on the client. Indicators for identifying a suspicious transaction/activity include the following:

- The client has an unusually comprehensive knowledge of money laundering issues and the AML/CFT/CPF Law without justification. For instance, if the client points out he/she wishes to avoid being reported.
- Attempt(s) to divide the amounts of any transaction thereby making the amount fall below the applicable designated threshold that would automatically trigger the reporting of the matter to the competent authorities regarding money laundering or terrorist financing suspicion.
- The client has an unusual interest in the internal policies, controls, regulations and supervisory procedures and unnecessarily elaborates on justifying a transaction.
- When a client has accounts with several international banks or has lately established relationships with different financial institutions in a specific country without clear grounds, particularly if this country does not apply an acceptable AML/CFT/CPF regime.
- The client is reluctant to provide the usual required information, or provides only minimal, false or misleading information. In addition, the information is difficult to verify.
- The client is reserved, anxious or reluctant to have a personal meeting.
- The client has an unusual or extremely nervous behaviour.
- The client uses different names and addresses.
- The client requests or seeks to carry out the transactions without disclosing his identity.
- The client requests that the transaction be completed within an expedited time period.
- The client refuses to submit original documentation, particularly those related to his physical identification or address.
- The client threatens/intimidates personnel in an effort to impede their duties.
- The client offers/suggests payment for a special favour or exemption.
- The client refuses to complete a Source of Funds Declaration Form.
- The client intentionally conceals certain important information like his address (actual place of residence), telephone number or gives a non-existent or disconnected telephone number.
- The client submits an overpayment of an invoice and request to have the amount returned via bank draft.
- An incoming wire followed by an immediate request for a withdrawal/refund.
- The client uses a credit card issued by a foreign bank that has no branch/headquarters in the country of residence of the client while he/she does not reside or work in the country that issued said card.
- Cash transactions where banknotes with unusual denominations are used.

NB* The presence of one or more of these indicators does not necessarily mean that money laundering or financing of terrorism is in fact taking place. The CO, upon the examination of the activity/transaction, must build conclusions on an objective basis and consider carefully all related conditions and evidence. In the event of possible suspicion, the client and their transactions/activities should be monitored to ensure adequate evidence is acquired to prove the offence or disregard the initial suspicion.

16.0 REPORTING OF SUSPICIOUS ACTIVITIES/ TRANSACTIONS

All personnel should be aware of their role and duty to complete and submit an internal Suspicious Transaction Report (STR) to the CO/RO when suspicion is noted during the course of their duties. The CO/RO would launch an internal investigation on the client's history and nature of transaction that would include a revision of the client's profile for any unusual activity/transaction.

The officer would build an internal report outlining the outcome of his/her investigation including the decision on whether or not to file an external STR with the FIU.

The internal Suspicious Transaction Report (STR) will contain at minimum the details of:

- The date of the report and the Officer who made the report;
- Personal particulars (name, identity card or passport number, date of birth, address, telephone number, bank account number) of the person(s) or company involved in the suspicious transaction;
- Details of the suspicious transaction/activity;
- The reason why the transaction/activity is suspicious - which suspicious activity indicators are present?
- The explanation, if any, given by the person about the transaction.

If the CO/RO suspects or has reasonable grounds to suspect that funds concerning an actual or proposed transaction/activity are the proceeds of any criminal activity or are related to money laundering or terrorist financing, the CO/RO shall file a written Suspicious Transaction Report (STR) with the Financial Intelligence Unit (FIU) in the prescribed form within twenty-four (24) hours of such determination or knowledge of forming the suspicion.

If the CO concludes that no external report should be submitted to the FIU, the justification of such a decision should be documented. All internal STRs should be maintained in a separate file by the CO/RO, whether or not an external STR is filed.

The CO/RO will maintain the Register of Suspicious Activity Reports (SARs) and/or Suspicious Transaction Reports (STRs) made to the FIU. The Register should contain details of the following:

- The date of the report;
- The person who made the report;
- The person(s) to whom the report was forwarded;
- A reference by which supporting evidence is identifiable; and
- Receipt of acknowledgment from the FIU.

All internal and external investigations conducted for suspicion noted must be kept confidential. It is a criminal offence to inform a client of an investigation or possible investigation or the filing of an STR with the FIU.

All STRs will be maintained for a minimum of five (5) years. In the event that the STRs submitted are under active investigation by the FIU and/or other relevant authority, these documents may be retained for a longer period of time until the investigation is completed and the case has been closed.

Enquiries from FIU and Other Competent Authorities

The CO/RO will maintain a separate register for all enquiries made to Regency by the FSRC, FIU or other local or non-local authorities. The register should contain the following details:

- The date and nature of the enquiry;

- The name and agency of the enquiring officers;
- The powers being exercised;
- Details of the account(s) or transaction(s) involved; and
- A list of any documents released.

The CO/RO is required to respond to or acknowledge the enquiries received within two (2) business days. Copies of all correspondence and/or information submitted to the relevant competent authorities should be retained within the Register of Enquiries.

17.0 EMPLOYEE TRAINING & KNOW YOUR EMPLOYEE (KYE) - RECRUITMENT/SCREENING/MONITORING

Employee Training

Money Laundering is an ever-evolving financial crime that constantly re-innovates itself; and as such, Regency is committed to implementing and enforcing all measures deemed necessary to prevent and/or mitigate all risks associated with money laundering, terrorist financing and proliferation financing as it relates to the operations of the business. In an effort to accomplish this Regency shall provide AML/CFT/CPF training to all personnel. This will ensure that they are adequately prepared for encounters with AML/CFT/CPF activities and that they remain current and aware of related evolving trends. Training for personnel, will be logged in a training register and records maintained.

All AML/CFT/CPF Training efforts are geared towards accomplishing the following objectives:

- To ensure that Regency has proper procedures in place to obtain the best possible training (whether internal or external) from qualified trainers that would provide pragmatic concepts that are applicable to the operations of the business.
- To thoroughly train personnel at all levels to proficiently fulfil their duties relevant to the nature of business conducted at the entity.
- To comply with jurisdictional legislation as well as best industry practice where there are no provisions made in current legislation.
- To stay updated with the industry's new trends and information that may impact/influence the operations of the entity.
- To heighten vigilance and equip personnel with the tools and skills necessary to prepare required reports such as STRs/SARs, and fulfil other functions essential to the operations of the entity.

The training provided to personnel will adequately cater to the operations of the business, its personnel and clients. The CO would continuously assess and analyze the business environment and operations to determine the training needs for personnel complement. An annual training schedule would be developed in line with these training needs.

The CO will liaise with the Executive Management Team to identify relevant training programs for all new personnel, which would include a comprehensive review of all policies and procedures of the business and the laws and regulations of St. Kitts and Nevis relevant to the business. This training program will be provided within 45 days of commencement of engagement. The CO and Executive Management will be subjected to immediate AML/CFT/CPF training upon assumption of duties.

Annual AML/CFT/CPF Training is compulsory for all personnel to ensure that they are kept informed and up-to-date with changes in the business and the business environment; changes in policies, procedures and international standards; risk vulnerabilities; and information on current AML/CFT/CPF techniques, methods and trends.

Upon completion of all training attended by Regency personnel, all persons are required to submit a copy of the certificate received for completion of the training which would be placed

on the respective personnel's human resource file. A copy of the material presented should also be given to Executive Management or the CO. In addition, all personnel are required to complete the Personnel Declaration on an annual basis to indicate that the AML/CFT/CPF Compliance Program Manual has been read/reviewed and understood.

For training conducted internally (typically by the CO), each person is required to complete a training record, outlining the particulars of the training received.

Know Your Employee (KYE) – Recruitment/Screening/Monitoring Procedures

As important as it is to "Know Your Customer/Client" with whom you conduct your business, it is equally important to "Know Your Employee" who is the first point of interaction with the new and existing clients.

Personnel are very vital components to the organization. They represent the organization's values and give it an identity. Their ethics and behaviour form part of the business' reputation, therefore, all personnel are required to conduct their duties in an honest and professional manner. In this regard, it is important that Executive Management and the CO have adequate knowledge and understanding of all personnel.

The following documents may be collected and reviewed prior to offering employment to a suitable candidate:

- Suitable copies of identification;
- A resume or curriculum vitae;
- Copies of professional and educational qualifications;
- Letters of reference;
- Proof of address; and
- A police certificate or criminal affidavit.

Upon employment, a human resource file would be developed for all personnel with the information outlined above in addition to:

- an engagement agreement or contract, as well as the job description;
- copies of training certificates;
- performance evaluations or appraisals;
- records of vacation;
- any disciplinary actions taken against any personnel; and
- any due diligence or background checks performed on any personnel.

Management would also conduct periodic evaluations on all personnel to ensure that their behaviour is in consistent with the ethics, policies and procedures of the business and that such behaviour does not give the appearance of suspicious conduct. The following factors will be considered:

- lifestyle and spending habits consistent with salary, financial position or level of indebtedness;
- sudden and significant change in standard of living;
- refusal to take vacation leave for no apparent reason;
- suspiciously regular receival of gifts and/or gratuities;
- insistence in servicing a particular customer;
- refusal to accept promotion or changes to activities assigned; and
- later than normal office hours or odd hour office visits.

18.0 AUDIT FUNCTION

The CO will, or will identify support personnel, properly and adequately trained in St. Kitts and Nevis AML/CFT/CPF, to be assigned the role of "Audit Inspector(s)".

The Audit Inspector(s) may conduct a review of Regency as per the terms of a review programme devised by the CO. The results will be reported to Executive Management.

19.0 INDEPENDENT AUDIT

Regency is aware that having an AML/CFT/CPF Compliance Program to meet local legislative requirements and international standards is not enough. The program must be continuously monitored and tested to ensure it remains relevant within a dynamic business. A systematic review and analysis must be conducted at least every two (2) years on the policies and procedures of the business to determine that these remain adequate, accurate and current, in accordance with the Laws and Regulations of St. Kitts and Nevis, and are efficient and effective in detecting money laundering and terrorist financing.

Regency shall appoint a suitably qualified auditor with the requisite competencies and professional ethics to audit its AML/CFT/CPF program in accordance with its risk management policies, at least every two (2) years. The appointed auditor shall be free from influence by Executive Management and personnel of Regency.

Regency will develop its audit plan using a risk-based approach which will be approved by Executive Management; the relevant persons will be notified of the audit and its duration. Any issues, deficiencies and/or weaknesses identified in the draft report provided by the independent auditor would be addressed and the relevant feedback provided by management in a suitable time-frame. The final report will thereafter be reviewed and approved by Executive Management and the auditor will conduct follow-up post audit to ensure (to the extent possible) that any inconsistencies noted in the report or delays in completion of recommendations have been addressed.

The appointed auditor will conduct the audit as prescribed by section 28A of the FSIISR. Any weaknesses identified by the auditor should be reviewed and monitored in a frequency and manner that will reduce or maintain Regency´s risk appetite.

20.0 GENERAL GUIDELINES TO COMPLIANCE & REVIEW OF THE MANUAL

All personnel of Regency who work with customers shall have a reasonable and general knowledge of the nature of the customer's particulars so as to be able to recognise suspicious activities.

Once a business relationship exists, personnel must remain vigilant so that they can recognise activities that are unusual within the context of their understanding of the customer's business.

Where verification of an applicant for business or customer remains incomplete for an unreasonable period of time, or is unsatisfactory, Regency may suspend the business relationship with that person and decline to perform further Fiduciary Services or Insurance Management Services on behalf of that person until such verification is satisfactorily completed.

This Manual will be reviewed by the CO on an annual basis to ensure that the developed policies and procedures remain current with the relevant legislation and international standards.

GLOSSARY:

"Beneficial Owner" refers to the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.

"Business Relationship" means an arrangement between two or more persons where:

(a) at least one of those persons is acting in the course of a business;

(b) the purpose of the arrangement is to facilitate the carrying out of transactions between the persons concerned on a frequent, habitual or regular basis; and

(c) the total amount of any payment or payments to be made by a person to any other person in the course of that arrangement is not known or capable of being ascertained at the time the arrangement is made.

"Caribbean Financial Action Task Force (CFATF)" is an FATF-Styled Regional Body (FSRB) made up of 27 states of the Caribbean Basin.

"Compliance Officer" means a senior officer designated by Regency to develop and implement the AML/CFT/CPF Compliance Program and ensure that the policies and procedures of Regency are in accordance with the required legislation.

1. Reference to "ultimately owns or controls" and "ultimate effective control" refer to situations in which ownership/control is exercised through a chain of ownership or by means of control other than direct control.
2. The definition should also apply to a beneficial owner or a beneficiary under a life or other investment linked insurance policy.

"Entity" means a company incorporated under the Companies Act, Cap 21.03 or the Companies Ordinance Cap. 7.06.

"Financial Action Task Force (FATF)" is an inter-governmental body established in 1989 by the Ministers of its Member jurisdictions.

"ISO 31000 Risk-Management Framework" is a risk framework that covers the essential aspects of risk management practices in organisations by providing a set of principles, a management framework, and a process that can be used to evaluate and further improve the organisation's risk management procedures.

"Person" includes a body corporate and unincorporated body.

"Politically Exposed Person (PEP)"

Foreign PEPs are individuals who are or have been entrusted with prominent public functions by a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials.

Domestic PEPs are individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials.

Persons who are or have been entrusted with a prominent function by an international organization refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions.

"Regulated Person" means any person carrying on a regulated business activity as defined under the Proceeds of Crime Act 4.28.

"Reporting Officer" means the individual responsible for receiving, considering and submitting the relevant reports/information to the FIU or any other competent authority regarding suspicion or suspicious activities/transactions.

www.regencyassurance.com
info@regencyassurance.com