THE COMPLIANCE COMMISSION OF THE BAHAMAS

THE INSURANCE COMMISSION OF THE BAHAMAS

Document for Consultation

GUIDANCE NOTE ON THE SOUND MANAGEMENT OF RISKS RELATED TO FINANCIAL CRIME IN THE BAHAMAS

The Central Bank of The Bahamas
Securities Commission of The Bahamas
The Insurance Commission of The Bahamas
The Compliance Commission of The Bahamas

Bank Supervision Department

Publication Date: April 16, 2018

Closing Date for Comments: May 1, 2018

TABLE OF CONTENTS

ACRONYMS

ACAMS	Association of Certified Anti-Money Laundering Specialists
AML/CFT	Anti-Money Laundering/Countering the Financing of Terrorism
AG	Attorney General
BCBS	Basel Committee on Banking Supervision
BO	Beneficial Owner
CFATF	Caribbean Financial Action Task Force
CBOB	Central Bank of The Bahamas
CCB	Compliance Commission of The Bahamas
CDD	Customer Due Diligence
CO	Compliance Officer
COSO	Committee for Sponsoring Organizations
CRS	Common Reporting Standards
DNFBPs	Designated Non-Financial Businesses and Professions
FATCA	Foreign Account Tax Compliance Act
FATF	Financial Action Task Force
FC	Financial Crime
FIU	Financial Intelligence Unit
GCB	Gaming Commission of The Bahamas
ICB	Insurance Commission of The Bahamas
INED	Independent Non-Executive Director
INR.X	Interpretive Note to Recommendation X
IO	Immediate Outcome
MER	Mutual Evaluation Report
ML	Money Laundering
MLRO	Money Laundering Reporting Officer
MTA	Money Transmission Agent
MTSA	Money Transmission Service Provider
NPO	Non-Profit Organization
NRA	National Risk Assessment
OAG	Office of the Attorney General
PEP	Politically Exposed Person
RBA	Risk-Based Approach
RBPF	Royal Bahamas Police Force
SCB	Securities Commission of The Bahamas
SFI(s)	Supervised Financial Institution(s)
SOF	Source of Funds
SOW	Source of Wealth
SRB	Self-Regulating Body
STR	Suspicious Transaction Report
TF	Terrorist Financing
UTR	Unusual Transaction Report(ing)

1 INTRODUCTION

1.1 Effective management of risks relating to financial crime is essential for the success and safety of SFIs and DNFBPs (collectively referred to herein as "licensees") in The Bahamas and the financial services sector as a whole. The ability to enter the proceeds of criminal activity into the financial system is the goal of criminal operations. According to the CFATF July 2017 Mutual Evaluation Report (MER), *"specific sectors are attractive either for the nature of the transactions or the limited nature of regulation. These include the international securities sector, dealers in precious metals and precious stones, money transmission services and attorneys"*.

1.2 The Financial Regulators in The Bahamas (collectively referred to as "the Regulatory Authorities") are providing this Guidance Note on the identification, assessment, management and mitigation of financial crime risk. The following Regulatory Authorities have agreed to participate:

(i) The Central Bank of The Bahamas ("CBOB") – responsible for the regulation and supervision of Bahamian banks, trust companies, co-operative credit unions and money transmission companies (collectively known as "supervised financial institutions" or "SFIs");

(ii) The Securities Commission of The Bahamas ("SCB") - a Statutory Body mandated to administer the various Securities and Investment Funds Acts and Regulations, with regulatory responsibilities for stock exchanges, brokers, broker-dealers, securities investment advisors and Financial and Corporate Service Providers operating in or from The Bahamas;

(iii) The Insurance Commission of The Bahamas ("ICB") - a Statutory Body responsible for the regulation and supervision of all insurance activity within or through The Bahamas. It is concerned with the ongoing monitoring and supervisory oversight of domestic and external insurers as well as intermediaries, including agents, brokers, salespersons, insurance managers; and

(iv) The Compliance Commission of The Bahamas ("CCB") - an independent Statutory Authority responsible for regulating DNFPBs to ensure compliance with the Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) rules and regulations found in the Financial Transactions Reporting Act, 2000 (FTRA); the Financial Transactions Reporting Regulations, 2000; and the Financial Intelligence (Transactions Reporting) Regulations 2001, and other substantive laws in The Bahamas, Codes of Practice and guidelines.

1.3 The Regulatory Authorities will not accept any arrangements in the financial system that might facilitate the free flow of proceeds to and in The Bahamas from criminal activity. The ability of licensees and other stakeholders to effectively identify, assess and manage risks related to financial crime at both the macro and micro levels is paramount to effectively impeding financial crime.

2. PURPOSE

2.1 In recent years, the financial services industry in The Bahamas began to transition from a compliance-focused regime where the emphasis was on strict adherence to the specified rules to avoid fines and other official sanctions, to a risk management-focused approach that recognizes that while rules must be adhered to, the underlying principle is that it is harmful to any firm, and a great harm to the Bahamian society and economy, to conduct business with financial criminals.

2.1 The purpose of this document is to provide guidance on the conduct of financial crime-related risk management at both the enterprise and client levels. It is intended to give adequate assistance to ensure that the goals and objectives of the FATF standards are met and to assist licensees in their attempts to detect when and reduce the likelihood that their institution will be involved in financial crime activities. The Regulatory Authorities and their licensees must include financial crime risks within their overall risk management regimes. The inadequacy or absence of sound financial crime risk management exposes licensees to serious risks, especially reputational, operational, compliance and legal risks (see *BCBS Guidelines for the Sound Management of Risks relating to ML & FT).*[1]

2.3 The Regulatory Authorities propose ten (10) core principles that licensees are to follow to suppress financial crime. These principles are outlined in section VII.

3. SCOPE

3.1 This Guidance Note should be read in conjunction with relevant domestic legislation, other standards, codes of practice and guidelines produced by the CBOB, SCB, ICB, and the CCB (collectively called "the Regulatory Authorities"), as well as by the relevant regulators in offshore jurisdictions, that are engaged in the supervision of single and multi-national SFIs and DNFBPs (collectively called "licensees") (*(ref BCP 12 in Core Principles for Effective Banking Supervision - 2012).* Many licensees in The Bahamas have clients with multiple relationships and/or accounts within the same Group, but located in offices spanning different countries. Accordingly, it is imperative that multi-jurisdictional licensees also have a Guidance Document that can be a reference tool in their global financial crime risk management efforts.

CORE FATF OBLIGATIONS AND DECISIONS REGARDING ML/TF RISK ASSESSMENTS

3.2 It is critical that the users of this Guidance Note understand the obligations contained in the FATF's *Recommendation 1* and its interpretive note, which speaks to countries, financial institutions ("FIs") and designated non-financial businesses and professions ("DNFBPs) identifying, assessing and mitigating ML and TF risks. For more details, reference should be made to the texts of *Recommendation 1* and its interpretive note (Appendix "D"), as well as the FATF assessment methodology. [2]

[1] ***https://www.bis.org/bcbs/publ/d353.pdf***

[2] www.**fatf**-gafi.org/media/**fatf**/documents/**recommendations**/pdfs/**FATF**

4 APPLICABILITY

4.1 Consistent with international and local standards, this Guidance Note seeks to inform the following entities and individuals:

(i) Policy makers and other authorities;

(ii) Regulators, supervisors and self-regulating bodies (SRBs);

(iii) SFIs and DNFBPs for which financial crime risk assessments at both macro and micro levels are critical to their risk based obligations;

(iv) Non-profit organizations (NPOs);

(v) AML/CFT assessors and assessment bodies, as well as academia, specified individuals, etc.; and

(vi) the general public.

5 WHAT IS FINANCIAL CRIME RISK MANAGEMENT?

5.1 The effective management of risks relating to Financial Crime relies on the identifying and measuring of inherent and residual financial crime risks that can potentially impact an institution, and the development mitigating measures that will ultimately assist in effective risk management (*see Appendix "D" attached for further definitions)*.

6 LEGISLATIVE & REGULATORY FRAMEWORK FOR SOUND FINANCIAL CRIME RISK MANAGEMENT

6.1 The Laws of The Bahamas that are specific to financial transactions, the proceeds of crime, anti-money laundering and countering the financing of terrorism, and by extension financial crime risk management, are set out in Appendix "A".

6.2 Regulatory Guidelines that address aspects of financial crime risk management are set out in Appendix "B".

7 TEN PRINCIPLES TO CONSIDER FOR SOUND FINANCIAL CRIME RISK MANAGEMENT

(i) PRINCIPLE I – INTOLERANCE TO FINANCIAL CRIME

7.1 Refusing to facilitate financial criminality is simply good business practice, and not just a necessity to avoid financial or regulatory sanctions. Policies, procedures and practices developed and maintained by regulatory authorities and their licensees must correspond with this principle. (ref. BCBS' updated "*Core principles for effective banking supervision (2012)",* and the *BCBS Sound Management of risks related to money laundering & terrorist financing, June 2017).* Regulatory authorities and licensees must focus on the prevention of

financial crimes within their operations, to further demonstrate a strict intolerance to financial crime. In addition to the actions required under Principle II herein, regulatory authorities and licensees may find that in addition to activities that seem suspicious, non-compliance of persons within their oversight should also be treated with strict intolerance at the earliest stage, prior to same becoming an avenue for financial crime.

(ii) PRINCIPLE II - RISK ASSESSMENT, MANAGEMENT & MITIGATION

7.2 Each licensee must adopt a risk-based approach rather than a solely compliance-based approach, in the administration, management and regulation of their licensees. The Regulatory Authorities are also mandating that all licensees adopt sound practices to mitigate Financial Crime risks relevant to their customers and operations. A risk-based approach exercises the principal of proportionality and is informed by the licensee's risk assessment of Financial Crime ("FC") risks. This document sets out guidance in respect to such measures. Additional guidelines (see appendices below) are applicable or supplementary where no specific FC Risk guidance exists.

7.3 Licensees should undertake an enterprise risk assessment exercise, using a four-pronged approach. Under this approach, inherent and residual risk factors should be identified and considered at the following levels:

(i) country
(ii) sectoral/industry
(iii) entity-specific; and
(iv) business relationship.

7.4 Regulatory Authorities also conduct AML/CFT risk assessments for each of their licensees, and seek to regularly update these.

I. Country Level (National Risk Assessment)

7.5 *The Bahamas' National ML & TF Risk Assessment (2015/2016) (NRA) Summary notes that "The FATF sets global AML/CFT standards. Foundational to this are the FATF's Recommendations, which mandate that countries undergo ML/TF risk assessments".* The NRA "represents the combined effort of more than a dozen public and private sector stakeholders" and the document seeks to provide information on ML/FT vulnerabilities at the national or country level. Stakeholders including licensees are urged to use this information to feed into their overall assessment of financial crime risks.

II. Sectoral Industry Level Risk Assessment

7.6 The NRA also identifies vulnerabilities and risks that are sector-specific. Licensees should take these into account where applicable, when conducting enterprise risk assessments.

III. Entity-Specific Level Risk Assessment

7.7 All licensees must undertake and document an appropriate entity-specific financial crime risk assessment, in concert with the assessment of all other inherent and external risks. It is vital that this exercise not be limited to ML and FT risks, but also encompass other areas of financial crime (examples include fraud and forgery) where applicable. This holistic exercise should shape the organization's risk profile and appetite, which should be documented, Board-approved, and reviewed and analyzed annually. Notwithstanding the scheduled annual review, the licensees' risk profile and appetite should also be reviewed on an ad-hoc basis by senior staff/Board members, if there are any sudden, material changes to the risk factors that were originally considered, or where new risk factors have been identified.

7.8 Analyzing, understanding, rating documenting and categorizing all inherent and external risks before offering a new service or product, and before marketing clients from outside the usual client profile, will produce the data necessary to implement effective policies and procedures. This includes due diligence, customer acceptance, and ongoing monitoring to adequately control identified inherent financial crime risks. Any resulting residual risk should be managed in line with the entity's risk profile established through its risk assessment.

IV. Relationship Level Risk Assessment

7.9 Pursuant to Section 5 of the FTRB 2018, each licensee must develop a risk assessment framework which is approved by its Board of Directors ("the Board"), to ensure appropriate measures are taken to identify, assess and mitigate its identified risks. This framework must be appropriate for the type of products offered by the licensee, and capable of assessing the level of potential financial crime risk each client relationship poses. Factors to be considered in developing this framework are listed in (but not limited to) the FTRB, AML/CFT Rules and Guidelines and Risk Assessment Framework of the Regulatory Authorities. All relationships must be risk rated/assessed. The ratings/assessment results must be documented and be replicable by other stakeholders such as compliance, internal audit and the Regulatory Authorities to ensure that the risk rating methodology has qualitative integrity and consistency

(iii) PRINCIPLE III - PROPER GOVERNANCE

7.10 The overall effectiveness of Financial Crime Risk Management and governance should be continuously monitored and periodically evaluated by the Board. Board Committees such as the Risk Management Committee and the Compliance Committee (particularly where the Board's INEDs are a part of these) can be used to monitor and periodically evaluate the overall effectiveness of the process, while keeping the full Board informed.

7.11 Principle 1 and 2 of the *BCBS Guidelines on Compliance and the Compliance Function in Banks*, describe the responsibilities of the Board and Senior Management. Principle 3 describes the need for a compliance policy that should be established, communicated and observed by all three lines of defense.

(iv) PRINCIPLE IV - THREE LINES OF DEFENSE

7.12 The three lines of defense approach to risk management are widely accepted as the global standard.[3]

First Line of Defense

7.13 The business units (or business lines) in licensees are regarded as the first line of defense. They are responsible for identifying, assessing and controlling the risks of their businesses. They should know all relevant policies and procedures and be allotted sufficient resources to carry them out effectively. This group should conduct regular control risk self-assessments (CRSAs), ranging from surprise cash counting for cash holding officers such as tellers in commercial banks, to identifying, assessing and mitigating key risk indicators (KRIs) in a broader context by quality assurance groups. The first line of defense is necessary, but it is important to remember that this line has competing priorities such as the need to earn revenue, while retaining and acquiring customers.

Second Line of Defense

7.14 The second line of defense provides independent oversight and independent quality assurance for the overall operations of the entity. Section 5.8 of the CBOB Corporate Governance Guidelines and the *BCBS Guidelines on Sound Management of Risks related to ML & TF* both speak to the independence of the CO and MLRO function(s) which, along with Business Risk, usually comprise this second line. These functions are expected to provide ongoing monitoring of FC risks, including sample testing, and review of exception reports. Their solid or straight reporting line should be outside the business line. Performance assessments for the individuals in this group should be undertaken by individuals or groups that are outside the business line.

Third Line of Defense

7.15 The third line of defense comprises the internal audit function and is vital to the independent evaluation of risk management and controls. This group discharges its responsibilities to the audit committee of the Board or a similar oversight body, through periodic evaluations of the effectiveness of compliance with policies and procedures related to FC. *The BCBS Sound Management of Risks* describes the audit function's role as the third line of defense.

External Auditors

[3] ***https://www.coso.org/Documents/COSO-2015-3LOD.pdf***

7.16 In The Bahamas, external auditors also play a critical role in evaluating the internal controls and procedures of most licensees in the course of their financial audits, and in confirming that they are compliant with AML/CFT regulations and supervisory expectations. Licensees that use external auditors to evaluate the effectiveness of AML/CFT policies, should ensure that the scope of the audit is adequate to address the licensee's risks, and that the auditors assigned to the engagement have the requisite expertise and experience (ref. *BCBS Guidelines - Sound management of risks related to ML &TF*).

(v) PRINCIPLE V – BOARD OVERSIGHT

7.17 The Board should regularly ensure that the licensee's financial crime risk management regime is commensurate with regulatory and industry standards, as well as its own risk profile and appetite. The Board should oversee current and potential risks, and the arrangements for their sound management, often via reports from the second and third lines of defense. Key areas for the Board to review and monitor (through the use of reports from all three lines of defense and other measuring tools) to ensure that the licensee is practicing effective FC risk management should include:

(i) Relationship & Customer Acceptance;
(ii) Ongoing Relationship & Transaction Monitoring;
(iii) Correspondent Banking;
(iv) Exception reporting (e.g. Report of Accounts with missing legislative documentation)
(v) Cash transactions; and
(vi) Suspicious transactions reporting.

(vi) PRINCIPLE VI – BUSINESS ACCEPTANCE

7.18 *Part II of the FTRA (Chapter 368)* speaks extensively to the licensees' legal obligation to verify client identities, as do SCB's Securities Industry (AML and CTF) Rules[4] and the new CDD and account opening guidelines annexed to the *CBOB AML/CFT Guidelines.* The latter describes the requirement of using independent source documents, in addition to customer attestations, to fulfill these legal mandates. For further references, the *BCBS' Customer Due Diligence for Banks* document and other relevant guidelines offered by the Regulatory Authorities should be consulted.

(vii) PRINCIPLE VII – ONGOING MONITORING

7.19 The majority of Bahamians and financial customers globally are not financial criminals, and ideally a licensee's risk management systems will be risk-based and not pose a significant inconvenience to law-abiding customers. The position of the Regulatory Authorities is that licensees should engage customers on the assumption that they are not criminals, while still considering this possibility. The principle of proportionality to the risk assessment of the client/product/jurisdiction will yield varying levels of compliance requirements. Cross-border

[4] ***www.scb.gov.bs/documents/FINAL%20-%20Amended%20SCB-AML%20Guidelines%20with%20merged%20Notice%20-%20%2011Aug2011PDF.pdf***

customers and transactions, and customers with large, complex, or high-risk financial arrangements, should receive enhanced due diligence to mitigate the financial crime risks.

7.20 Once the relationship has been risk rated according to the risk rating framework established by the institution, due diligence must be applied *that is commensurate with the level of risk associated with the relationship*.

7.21 **For relationships deemed lower risk, simplified measures are appropriate** (*ref. CBOB AML-CFT Guidelines).* Although institutions may opt to apply a due diligence methodology that is consistent across all risk types, this may result in a denial of access to financial services by individuals who are financially and socially disadvantaged, with the unintended result of further increasing the risk of financial crime in the jurisdiction.

7.22 For higher risk-rated relationships or clients, enhanced measures are to be taken to mitigate and manage those risks, if the decision is made to pursue a business relationship from such clients. To avoid offences as described in Section 12 of the FTRA, licensees are to employ enhanced due diligence measures at the commencement of the business relationship, and continually for the duration of that business relationship if the risk remains heightened. This typically includes an extensive, formal review of the risks conducted at least annually. Foreign PEPs, relationships with large account balances and those who conduct regular cross-border transactions are just some of the examples of the relationship types that fit into this category. Increased scrutiny and enhanced due diligence are to be employed with such clients.

7.23 The licensee's customer acceptance policy should also define circumstances under which a new business relationship cannot be accepted or under which an existing one should be terminated. A new business relationship should not be established if the product provider is unable to complete its CDD measures.

7.24 The above references are consistent with *FATF Recommendation 10*, and consistent with FATF standards, procedures which mandate the verification of identity of the beneficial owner, using reliable, independent source documents, data, or information. The approach employed by the licensee must be risk-based, and this information must be used to build an understanding of the relationship – its profile and behavior. The purpose of the relationship (or the occasional transaction where applicable), the expected level of assets, expected average size of the transactions, and the expected regularity of transactions must be documented at the outset, and periodically matched against actual numbers once the relationship is operational. Any material deviation from activity or behavior considered "expected" must be identified for further review. Such profiles assist in the ever-greening of the risk ranking of relationships. They also help the licensee to decide on the future handling of the relationship, or indeed whether to terminate or de-market it.

7.25 The Regulatory Authorities agree that risk assessments are required for other entities and transactions, such as:

(a) ELIGIBLE INTRODUCERS & OTHER INTERMEDIARIES

7.26 In accordance with the CBOB AML-CFT Guidelines, it is expected that a risk review of all intermediaries (including business introducers) be conducted no less than annually, to ensure that the risk of doing business with the entity has not escalated over time to an unacceptable level.

(b) FIDUCIARIES

7.27 Licensees must:

(i) determine the general nature, purpose and SOF/SOW of the structure;
(ii) conduct enhanced due diligence on, and obtain and verify ID for the settlors, and any other person(s) who can:
- dispose of, advance, lend, invest, pay or apply trust property;
- vary the trust;
- add or remove a person as a beneficiary, or as a class of beneficiaries;
- appoint or remove trustees; and
- direct, withhold consent to or veto the exercise of a power.

(iii) obtain ID evidence for BOs, in the case of a nominee relationship.

7.28 Where any of the aforementioned is a legal person rather than a natural person, the corporate documents must be obtained, with proof of current registration. In addition, the enhanced due diligence employed must identify the natural persons behind the corporations used in the trust relationship.

(c) CASH TRANSACTIONS

(a) <u>International Banks and Trusts</u>

7.29 International banks and trusts active in The Bahamas do not as a matter of business practice, accept currency for deposit or investment. CBOB is consulting on whether it should formally ban acceptance of currency by these licensees.

(b) <u>Commercial Banks</u>

7.30 Commercial banks must conduct risk analyses when cash is first introduced by a client, if a customer has an occasional cash transaction that is larger than industry standards (currently $1,000.00 for MTBs and $15,000.00 for commercial banks) or any amount that is suspect, as well as for the ongoing management of any cash intensive relationship.

(d) CORRESPONDENT BANKING

7.31 Banks must gather enough information about their respondent banks to understand fully the nature of the respondent's business. When performing due diligence on correspondent banks, the risk rating methodology should include:

(i) conducting adequate and appropriate enhanced screening of the bank, such as an assessment of the respondent bank's management, and major business activities;

(ii) investigating and determining whether the foreign bank itself offers correspondent accounts to other foreign banks (e.g., nested accounts);

(iii) identifying the location and nature of the major business activities and customers of the foreign correspondent bank (knowing your customer's customers – KYCC) and performing enhanced due diligence as required;

(iv) identifying the owners, beneficial owners, and principals of the foreign bank if its shares are not publicly traded;

(v) ascertaining its money laundering prevention and detection efforts and the purpose of the account; and

(vi) determining the condition of bank regulation and supervision in the respondent's country.

7.32 In The Bahamas, shell banks are not permitted *(see Appendix "D" below for definition*).

(e) ONGOING RELATIONSHIP AND TRANSACTION MONITORING

7.33 Monitoring systems should be robust enough to immediately detect any material changes in the transactional profile of any customer, across any licensee's network of locations, to enable the business line and the MLRO to take appropriate and expeditious action if warranted. The systems should also allow the licensee to gain a centralized knowledge of information to initiate a trend analysis if necessary on any client (ref. *BCBS Guidelines on Sound Management related to ML & TF Risks).*

(f) ELECTRONIC FUNDS TRANSFERS

7.34 The *FATF's Recommendation 16* seeks to make both cross-border and domestic electronic funds transfers more transparent, so that law enforcement officials have an easier time tracing funds transferred electronically by money launderers, terrorists and other criminals. In The Bahamas, the *Financial Transactions Reporting (Wire Transfers) Regulations, 2015* seeks to implement the requirements of Recommendation 16.

7.35 Licensees should monitor wire transfers to and from higher risk countries or jurisdictions, as well as transactions with higher risk countries or jurisdictions, and suspend or reject wire transactions with sanctioned parties, or countries, or jurisdictions listed in Orders issued pursuant to the International Obligations (Economic and Ancillary Measures) Act, 1993 (CBOB AML-CFT Guidelines). A simplified due diligence approach for cross-border wire transfers is acceptable (usually for transfers below $1,000.00 if no other risks are evident), versus the usual medium diligence or even enhanced due diligence, (for transfers over $1,000.00 or when other risks are more likely).

(g) MONEY TRANSMISSION BUSINESSES ("MTBs")

7.36 MTBs are categorized as SFIs. Unlike other SFIs, however they often have a fleeting relationship with their customers, which make them vulnerable to ML and TF. As such, a

comprehensive FC risk program must be in place for such entities that are mandated to effectively manage these special risk factors.

(h) PARAMETER AND THRESHOLD BREACHES

7.37 Transactions which are incompatible with a licensee's knowledge and experience of the customer in question, or with the purpose of the relevant business, or have breached the parameters established for the relationship, warrant an investigation by senior management and potentially, by the MLRO. It may be determined by senior management or by the MLRO function that another full risk assessment of the relationship is warranted.

(i) UNUSUAL AND SUSPICIOUS TRANSACTION REPORTING

7.38 Policies and procedures must be in place to identify, investigate, and report suspicious transactions to the FIU. These policies and procedures must be communicated to all personnel during training.[5]

7.39 To avoid the offence of "Tipping Off" (see *Appendix "C"* for definition), avoid alerting any legal or natural person that he/she/the firm is being reported, or even investigated.

(viii) PRINCIPLE VIII – DE-MARKETING

7.40 Broadly speaking, licensees should terminate relationships and refuse business with any client who the licensee reasonably suspects is involved in financial crime. There are a number of specific requirements when licensees uncover evidence of financial criminality.

TERRORIST FINANCING AND ASSET FREEZING

7.41 The Proceeds of Crime Bill makes provision to cover all identified risks — money laundering, terrorism financing, terrorism, corruption, proliferation of weapons of mass destruction, human trafficking, virtual currencies – digital representation of value which can be digitally traded – and other factors that the Minister, by regulations, may recommend. There have been several incidents over the years where proceeds suspected to originate or be purchased from the sale of illegal drugs were confiscated.

7.42 Terrorist financing (including proliferation financing) on the other hand, is seen in The Bahamas as low risk, and there has been no record of domestic freezing decisions made by the competent authorities relative to this crime. Funds that are used to fund terrorist financing activities may be derived either from criminal activity or legitimate sources, depending on the type of terrorist organization involved. SFIs and DFNBPs must be able to detect and identify potential TF transactions. Although a risk-based approach is taken with the assessment of new business from a KYC perspective, irrespective of the risk rating assigned to the customer, **all** customers (new and existing) must be screened against lists of known or suspected terrorists issued by competent (national and international) authorities. (*see*

[5] ***laws.bahamas.gov.bs/.../FinancialTransactionsReportingAct_1.pdf***

Appendix "C" for definition). Automatic screening systems are allowed, but they must be adapted and modified to suit this purpose for each regulated entity. It is expected that Credit Unions who do not routinely onboard foreign nationals, for example, may take a simplified approach and use manual lists where applicable.

Closing suspicious accounts

7.43 Licensees are expected to have in place policies and procedures governing account closing, or de-marketing a relationship. The transaction records, including the documented customer due diligence material, must be kept for a minimum period of five (5) years after the last transaction on the account has been completed.

RECORD KEEPING

7.44 To enable investigating authorities to compile a satisfactory audit trail for suspected laundered money or terrorist financing and to be able to establish a financial profile of any suspect account/facility, the FTRA requires licensees to retain customer identification and transaction records for use as evidence in any financial crime investigation. Relevant records are critical to the success of such investigations, particularly where the financial criminal has attempted to confuse the audit trail by using complex layering techniques. All transactions effected via the SFI must be able to be reconstructed, all AML/CFT policies observed and court orders or enquiries from the appropriate authorities satisfied.

7.45 Records must be retained for at least five years after:

a. The carrying out of a one-off transaction or the last transaction in the series of transactions; and

b. The date a business relationship ends, or the date an individual ceases to be a facility holder i.e., the closing of the account or accounts;

MISCELLANEOUS FINANCIAL CRIMES

7.46 Although the following list is not exhaustive, and money-laundering risk is the most common financial crime risk factor that must be managed by licensees operating in The Bahamas, some of the other common financial crime risks that must be identified, assessed, managed and mitigated include:

(I) PROLIFERATION & PROLIFERATION FINANCING RISK

7.47 Information to manage and mitigate this risk can be found in the CBOB *Proliferation & Proliferation Financing Guidelines.*

(II) BRIBERY & CORRUPTION RISK

7.48 Licensees are exposed to Bribery & Corruption Risk through the activities of one or more of its clients, staff or third parties. CBOB *Corporate Governance Guidelines* give guidance to Board members to identify, monitor, and manage potential conflicts of interest of Board

members, management and significant shareholders, and abuses in related party transactions, as well as an overall process to monitor adherence to established standards of business conduct and ethical behavior. Additionally, licensees should assess overall corruption risk by the risk ranking of jurisdictions, and the risk ranking of industries which may be prone to bribery and corruption, by researching the FATF's Sensitive Jurisdiction List. When PEPs are involved, the jurisdictional risk is heightened, so licensees are expected to identify and assess all PEPs and risk-rate them appropriately.

(III) TAX EVASION RISK

7.49 The implementation of FATCA and CRS are anticipated to assist in the mitigation of tax evasion risks; however, all licensees must have controls to mitigate the risks of tax evasion, such as evidence that tax returns were filed by customers where applicable. During the onboarding process, licensees should consider undertaking a global tax review on each potential international customer and require these potential customers to complete tax declarations prior to finalization of the onboarding process.

(IV) CYBER CRIME RISK

7.50 Fraud perpetrated through false or misleading electronic data transmissions via computers, networks and other electronic mediums (Cyber Crime) is becoming more prevalent globally, and incidents have become more commonplace in all countries, including The Bahamas. The *CBOB Technology Risk Guidelines* stress the need for licensees to mitigate Data Security and Cyber Crime risks by:

(i) establishing a sound and robust technology risk management framework;
(ii) strengthening system security, reliability, availability and recoverability; and
(iii) emphasizing the benefit of using appropriate technologies and control mechanisms that protect customer data and transactions.

7.51 The CBOB *Technology Risk Guidelines* give further detailed and comprehensive instructions on managing and effectively mitigating the risk of cybercrime.

(ix) PRINCIPLE IX - TRAINING

7.52 It is imperative that employees and contractors are honest, well-trained and resolute in managing financial crime risks.

7.53 Timing and content of training for various sectors of staff should be based on the risk profile of the institution and adapted by individual institutions for their own needs. The *FTRR, 2001* requires that at least once per year, licensees shall provide relevant employees with appropriate training in the recognition and handling of transactions carried out by persons who may be engaged in money laundering.

7.54 The ICB's AML/CFT Guidelines state that "insurance companies must take appropriate measures to familiarize all employees with:

(i) policies and procedures designed to detect and prevent money laundering including those for identification, record keeping and internal reporting, and any legal requirements in respect thereof; and

(ii) training programs which incorporate the recognition and handling of suspicious transactions".

7.55 It is recommended that:

I. *New employees* who will be dealing with customers or their transactions (irrespective of their level of seniority) be given general ML/TF information within the first month of their employment. This general information should include a basic training course on money laundering and terrorist financing including relevant typologies and the need for reporting any unusual, inexplicable and suspicious transactions to the MLRO. New employees should also be provided with a copy of the written AML/CFT policies (including policies governing UTRs and STRs) and procedures and be made aware of the statutory obligation to report suspicious matters

II. *Front line staffs (including account/facility opening personnel)* who are dealing directly with the public are the first point of contact with potential money launderers and terrorist financiers, so they are vital to the organization's reporting system for suspicious transactions. They should be well versed in all aspects of KYC, AML and CFT procedures, as well as procedures dealing with one-off or occasional transactions. Training should also emphasize the need for and the methodology to verify identity, and on the financial institution's customer/client verification procedures. Training should be provided on factors that give rise to suspicions and the procedures to be adopted when a transaction is deemed suspicious. Front line staff should be made aware of their financial institution's policy for dealing with non-clients.

III. *Administrative/Operational Supervisors and Managers/Board of Directors* who are responsible for the book of business, supervising or managing staff should receive a higher level of instruction covering all aspects of AML/CFT procedures. These will include the offences and penalties for non-reporting and assisting money launderers arising from the POCA and FTRA, procedures relating to the service of production and restraint orders, internal reporting, identity verification, record retention and the disclosure of STRs under the FIUA 2000.

IV. *MLROs and COs* require in-depth training concerning all aspects of the legislation, regulatory guidelines and internal policies. Additionally, these functions require extensive initial and ongoing instructions on the validation, investigation and reporting of suspicious transactions, on feedback arrangements and on new trends and patterns of criminal activity.

7.56 Refresher training for *all* employees should be conducted at least annually to further manage and mitigate financial crime-related risks.[6]

[6] ***The Financial Intelligence (Transactions Reporting) Regulations, 2001***

Additional Licensee Training Requirements for Financial Crime specific to ICB:

7.57 It is encouraged that timing and content of AML/CFT training be adapted by individual insurance companies given the various sectors in which staff are exposed to their AML responsibilities.

Training Institutions

7.58 The primary training institutions utilized by regulators and licensees in The Bahamas to obtain AML and CFT specialized training for their management and staff are:

- The Association of Certified Anti-Money Laundering Specialists ("ACAMS") which offers a series of web-based, online courses, and which includes an online course to attain the internationally recognized Certified Anti-Money Laundering ("CAMS") professional designation; and
- The Bahamas Institute of Financial Services ("BIFS") which offers face to face, instructor-led classes to attain the UK based International Compliance Association ("ICA") Diploma.

The Regulatory Authorities view both ACAMS and BIFS as high quality institutions and accept the certifications from both of them. There is no particular preference held between these two institutions.

(x) PRINCIPLE X – IMPROVING FINANCIAL CRIME DEFENSES BY IMPLEMENTING CROSS-BORDER/GROUP WIDE FINANCIAL CRIME RISK MANAGEMENT

7.59 Many licensees in The Bahamas are global in nature, and the majority of parent companies or Head Offices are located in foreign jurisdictions. Hence, it is imperative that local policies and procedures comply with the more conservative of group policy or the relevant laws, regulations, and guidelines in The Bahamas. Where introducers and other intermediaries are used, licensees must ensure that these entities are subject to standards that are at least as strict as those governing their own FC Risk Management procedures.

GOVERNANCE AND RISK MANAGEMENT

7.60 Head Offices of financial groups must have access to relevant information to effectively develop, apply and enforce group policies and procedures relative to FC, and customer relationships and activities must be monitored on a consolidated basis. Consideration of host country legal requirements is also imperative. Relevant policies and procedures must be appropriately strengthened where necessary to take into account, local business considerations and special legislative and regulatory requirements in the host jurisdiction.

7.61 A thorough understanding of all the risks associated with a customer across the group is fundamental in developing an effective consolidated risk management regime.

THREE LINES OF DEFENSE IN THE CONTEXT OF INTERNATIONAL OR CONSOLIDATED RISK MANAGEMENT

(i) First Line

7.62 It is imperative that the global standard of the three lines of defense remain pervasive throughout the organization's operations, even at the consolidated level. It is a usual practice for quality assurance teams from head office to supplement the first line of defense effort (usually demonstrated at the local level by the use of risk and control self-assessments ("RCSAs") by conducting reviews to ensure that products, services, practices and compliance are all within the Group's international standards and meet or exceed local standards.

(ii) Second Line

7.63 A bank performing business nationally and abroad should appoint a chief AML/CFT officer for the whole group (group AML/CFT officer). As part of global risk management, the group AML/CFT officer has responsibility for creating, coordinating and group-wide assessment of the implementation of a single AML/CFT strategy (including mandatory policies and procedures and the authorization to give orders for all branches, subsidiaries and subordinated entities nationally and abroad (ref. BCBS Guidelines on the Sound Management of Risks.)

(iii) Third Line

7.64 Group internal audit assumes this responsibility, driven by an audit scope and plan that takes into account the licensee's internal global risk appetite, external threats, as well as entity risk assessments at the local level.

GROUP WIDE INFORMATION SHARING

7.65 The Banks & Trust Companies Regulation Act, 2000 *(the "BTCRA")* imposes a duty of confidentiality on all licensees of the Central Bank of The Bahamas. There are limited exceptions to this confidentiality provision. Further, under the *Data Protection (Privacy of Personal Information) Act, 2003*, (the "*DPA*") imposes restrictions to safeguard and protect personal information of living individuals.

7.66 A licensee's group-wide policies and procedures must take into account the above referenced issues and obligations related to local data protection and bank secrecy laws and regulations. One common practice to address this challenge is to have information sharing clauses built into account opening documents and service level agreements with third (or related) party service providers.

MULTI-SECTORAL FINANCIAL GROUPS

Regulatory Perspective

7.67 The CBOB and the SCB have developed and documented a joint protocol for onsite examinations of their shared licensees (banking groups engaged in both banking and/or fiduciary business, and trading (discretionary and non-discretionary). This has included the development of a supervisory college comprised of the CBOB, SCB, and the ICB to jointly supervise an entity licensed by all three regulators, as envisaged by FATF Recommendation 26. Penalties regimes have been revamped and strengthened by the Regulatory Authorities to encourage licensees to refocus their efforts on mitigating FC risks across their groups.

Enterprise Perspective

7.68 The BCBS' Guidelines on the Sound Management of Risks related to ML & TF give guidance to financial groups offering a consortium of mixed services and products. They are required to have adequate financial crime risk management methodologies in place, to monitor and share information on the identity of their customers, their transactions and account activities across the entire group. This helps them to be cognizant of customers that use the groups' services across different sectors and jurisdictions.

OUTSOURCING FINANCIAL CRIME RISK FUNCTIONS

7.69 Functions outsourced to third party (or even related party) vendors should be documented in detail in Service Level Agreements ("SLAs"), duly approved by the Board and reviewed by the relevant supervisory agency, *prior* to the commencement of the outsourced arrangement. Due to legislative restraints, some FC risk functions cannot be outsourced, (e.g. the local MLRO function).

7.70 While there should be an established SLA in place, allowance of outsourced functions should be documented in the Guidelines, Codes of Practice and Regulations of the respective Regulatory Authorities.

CONTROL FUNCTIONS

7.71 The Control Functions used in the mitigation of Financial Crime Risks are found in Annex II.

APPENDIX A

The Proceeds of Crime Act, 2000 ("POCA") (as amended)

The purpose of this Act is to empower the Police, Customs and the Courts in relation to money laundering, search, seizure and confiscation of the proceeds of crime, and for connected purposes.

The Financial Transactions Reporting Act, 2000 ("FTRA") (as amended)

This Act imposes certain obligations on financial institutions in relation to the conduct of financial transactions; and for connected purposes.

The Financial Transactions Reporting Regulations, 2000 ("FTRR") (as amended)

This Act imposes certain obligations on financial institutions to verify the identity of an individual or person or corporation doing business in The Bahamas.

The Financial Intelligence Unit Act, 2000 ("FIUA") (as amended)

This Act governs the agency responsible for receiving, analyzing, obtaining and disseminating information which relates to or may relate to the proceeds of the offences in the Proceeds of Crime Act and Anti-Terrorism Act.

The Financial Intelligence (Transaction Reporting) Regulations, 2001 (as amended)

This Act imposes certain obligations on financial institutions in relation to the conduct of financial transactions; and for connected purposes.

The Anti-Terrorism Act, 2004 (as amended)

The Anti-Terrorism Act, 2004 defines the offence of terrorism and criminalizes the financing of terrorism. It applies to actions, persons and property both inside and outside The Bahamas. Persons who have reasonable grounds to suspect that funds or financial services are related to or are used to facilitate terrorism have a duty to report their suspicions to the Commissioner of Police. Failure to make a report is an offense. The Anti-Terrorism Act contains provisions empowering the Attorney General to freeze, forfeit and dispose of funds used to facilitate terrorism.

The Anti-Terrorism Act has adopted the International Convention for the Suppression of Terrorist Bombings, adopted by the General Assembly of the United Nations on 15th December, 1997. The Anti-Terrorism Act has adopted the International Convention for the Suppression of the Financing of Terrorism, adopted by the General Assembly of the United Nations on 9th December, 1999.

The Financial Transactions Reporting (Wire Transfers) Regulations, 2015

These regulations outline the protocol for institutions when transferring funds and identifying the payer of the transaction as stipulated in Section 11(1) of the Act and the Financial Transaction Reporting Regulations.

The Financial Transactions Reporting Act ("FTRA"), amended 2017

An Act to repeal and Replace the Financial Transactions Reporting Act and for Matters connected Thereto.

The Proceeds of Crime Bill ("POCB"), 2017

A Bill for an Act to Consolidate and Strengthen Measures to Recover the Proceeds and Instrumentalities of Crime and to Combat Identified Risk.

The Securities Industry (Anti-Money Laundering and Countering the Financing of Terrorism) Rules, 2015

The purpose of this Act is to ensure the securities industry in The Bahamas remains in compliance with international standards regarding anti-money laundering and countering financing of terrorism legislation.

The Compliance Commission of The Bahamas' Codes of Practice for Lawyers, Accountants and Real Estate Brokers & Developers

The Codes of Practice are intended to provide the respective Designated Non-Financial Business and Profession falling within the supervisory remit of the Commission with practical guidance as to the obligations, requirements, and standards to be complied with, for full adherence to the substantive laws in The Bahamas relating to Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT). It also supports the regulatory objective of maintaining the reputation of The Bahamas as a first-class international business centre with zero tolerance for criminal activity.

APPENDIX B

CBOB Corporate Governance Guidelines

These Guidelines governs the processes, structures and information used for directing and overseeing the management of an organization. Corporate governance provides the structure through which the objectives of the organization are determined, the strategies by which those objectives are developed and implemented, and the means by which the performance of the organization to achieve those objectives is monitored and controlled.

CBOB MLRO Guidelines

The scope of these Guidelines covers all mainstream fiduciary, banking, lending and deposit taking activities of Central Bank licensees. The Guidelines incorporate both the mandatory minimum requirements of the AML/CFT laws of The Bahamas and industry best practices. All SFIs of the Central Bank must pay due care to these Guidelines in developing responsible procedures suitable to their business to prevent money laundering and terrorist financing.

CBOB Non-bank MTSV & MTA Guidelines, amended March 2012

This Guideline specifies the major considerations of the Central Bank in assessing applications for licensing providers, registering agents and the information that would normally be required in support of such applications. It also set out the prudential, reporting and other regulatory requirements for providers and agents incorporated in The Bahamas. A crucial objective of the Central Bank is to ensure that providers and money transmission agents engage the proper internal systems, policies and controls to guard against perpetrators of money laundering and terrorist financing.

FATF Recommendations

The FATF Recommendations set out a comprehensive framework of measures which countries should implement in order to combat money laundering and terrorist financing, as well as the financing of proliferation of weapons of mass destruction.

FATF National ML and TF Risk Assessment, February 2013

A national risk assessment provides useful information to financial institutions and designated non-financial businesses and professions (DNFBPs) to support the conduct of their own risk assessments. It also serves as a framework for assessing ML/TF risks at the national level.

Basel Guidelines on Sound Management of Risks related to ML/TF

These Basel Guidelines promotes sound ML/TF risk management, in particular, for the overall safety and soundness of banks and of the banking system. It helps protect the reputation of both banks and national banking systems by preventing and deterring the use of banks to launder illicit proceeds or to raise or move funds in support of terrorism. Additionally, it preserves the integrity of the international financial system as well as the work of governments in addressing corruption and in combating the financing of terrorism.

ICB AML/CFT Guidelines for Insurance Companies

These Guidelines are intended to provide insurance companies with practical guidance and examples of good practice on how to implement the requirements of the AML legislation. This

supports the regulatory objective of maintaining the reputation of The Bahamas as a first-rate international financial center with zero tolerance for criminal activity.

Financial and Corporate Service Providers Handbook and Code of Conduct

This Code is intended to provide FCSPs with practical guidance and examples of good practice on how to implement the requirements of the AML legislation. It also supports the regulatory objective of maintaining the reputation of The Bahamas as a first-rate international business center with zero tolerance for criminal activity.

APPENDIX C

COMMONWEALTH OF THE BAHAMAS NATIONAL MONEY LAUNDERING AND TERRORIST FINANCING RISK ASSESSMENT SUMMARY 2015/2016
http://www.scb.gov.bs/documents/Bahamas%20NRA%20Summary%20of%20Key%20Findings.pdf

FATF GUIDANCE – NATIONAL MONEY LAUNDERING AND TERRORIST FINANCING RISK ASSESSMENT – dated February 2013
www.fatf-gafi.org/.../images/National_ML_TF_Risk_Assessment.pdf

INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION – The FATF RECOMMENDATIONS – updated November 2017
www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF

BASEL COMMITTEE ON BANKING SUPERVISION – GUIDELINES ON SOUND MANAGEMENT OF RISKS RELATED TO MONEY LAUNDERING AND FINANCING OF TERRORISM
https://www.bis.org/bcbs/publ/d353.pdf

EVERAGING COSO AGAINST THE THREE LINES OF DEFENCE
https://www.coso.org/Documents/COSO-2015-3LOD.pdf

FINANCIAL TRANSACTIONS REPORTING ACT
http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/2000/2000-0040/FinancialTransactionsReportingAct_1.pdf

FATF 40 RECOMMENDATIONS (Amended 2012)
www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf

BASEL SOUND MANAGEMENT OF RISKS RELATED TO MONEY LAUNDERING AND FINANCING OF TERRORISM (2017)
https://www.bis.org/bcbs/publ/d405.htm

BASEL CORE PRINCIPLES FOR EFFECTIVE BANKING SUPERVISION *(*2012)
https://www.bis.org/publ/bcbs230.htm

CFATF MUTUAL EVALUATION REPORT
https://www.cfatf-gafic.org/index.php/documents/cfatf-mutual

THE CENTRAL BANK OF THE BAHAMAS RISK BASED SUPERVISORY FRAMEWORK
www.centralbankbahamas.com/download/095314300.pdf

THE INSURANCE COMMISSION OF THE BAHAMAS RISK BASED SUPERVISORY FRAMEWORK
https://www.bahamas.gov.bs/wps/wcm/connect/1ccd2bee-30f1-482c-ad9f

CBOB AML/CFT GUIDELINES
www.centralbankbahamas.com/legal_guidelines.php?cmd=view&id=16242

BCBS GUIDELINES ON COMPLIANCE AND THE COMPLIANCE FUNCTION IN BANKS
https://www.bis.org/publ/bcbs113.htm

THE OFFICE OF THE SUPERINTENDENT OF FINANCIAL INSTITUTIONS ("OSFI") IN ITS LEGISLATIVE COMPLIANCE MANAGEMENT ("LCM") ***The Office of the Superintendent of Financial Institutions ("OSFI")*** **in its** ***Legislative Compliance Management (LCM)***
www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/gl-ld/Pages/e13.aspx

THE BCBS' CUSTOMER DUE DILIGENCE FOR BANKS
https://www.bis.org/publ/bcbs85.pdf

FATF – GUIDANCE FOR A RISK-BASED APPROACH - THE BANKING SECTOR – OCTOBER 2014
www.fatf-gafi.org/.../reports/Risk-Based-Approach-Banking-Sector.pdf

APPENDIX D

In discussing financial crime risk and its assessment, it is important to have the following common understanding of certain terms and concepts that are used throughout the Guidance Note:

Regulatory Authorities Regulatory Authorities refer to all regulators with designated responsibilities for licensees and registrants mandated to identify, assess, manage and mitigate all financial crime risks, including money laundering and/or terrorist financing. In the Bahamas, this includes the Central Bank, Securities Commission, Compliance Commission, Insurance Commission of The Bahamas, and others. These authorities are responsible for licensing, regulating, supervising and administering legal and natural persons that fall under their legal authority.

Licensees Licensees are natural or legal persons who are supervised by one or more of the above noted Regulatory Authorities and conduct, licensed and registered business for or on behalf of a customer. These include registrants particular to the ICB, SCB and the CCB.

Enterprise Risk Assessment The identification and assessment of all inherent and external risks that may affect a licensee.

Enterprise Risk Management ("ERM") The Committee of Sponsoring Organizations ("COSO") describes ERM as "a process, effected by an entity's board of directors, management and other personnel, applied in strategy-setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the agreement of entity objectives".

Shell Banks A shell bank is a financial institution that does not have a physical presence in any country. In order to prevent money laundering, Subtitle A of the USA PATRIOT Act specifically prohibits such institutions, with the exception of shell banks that are affiliate of a bank that has a physical presence in the U.S. or if the foreign shell bank is subject to supervision by a banking authority in the non-U.S. country regulating the affiliated depository institution, credit union, or foreign bank

Money Transmission Businesses ("MTBs") **Money transmission business (or service)** is the business of accepting cash, cheques, other monetary instruments or other stores of value in one location and the payment of a corresponding sum in cash or other form to a beneficiary in another location by means of a

	communication, message, transfer or through a clearing network to which the money transfer business belongs. Remittances may be domestic or international
Tipping Off	Any person who discloses to any other person, information or any other matter, which is likely to prejudice an investigation.
Competent (national and international) authorities	Competent Authorities refers to all public authorities with designated responsibilities for combating money laundering and/or terrorist financing and /or proliferation financing. In the Bahamas, this includes the Central Bank, Securities Commission, Compliance Commission, Insurance Commission of The Bahamas, RBPF, FIU and others. Internationally, they may include The Federal Reserve System, FATF, International Monetary Fund (IMF),, US Federal Bureau of Investigation (FBI), U.S. Department of Homeland Security (DHS) and others. These authorities are responsible for investigating and/or prosecuting money laundering, associated offences, terrorist financing, seizing/freezing and confiscating criminal assets as well as proliferation financing.
Supervisory College	Supervisory colleges are joint meetings of interested regulators with each other and/or with licensee officials concerning a shared licensee, and include detailed discussions about the inherent and residual risks that impact the licensee and any mitigating controls employed.
Inherent Risk	The risk exposure in a regulatory authority or licensee prior to implementation of steps or control measures taken to prevent and reduce the likelihood of financial crime.
Residual Risk	The risk exposure in a regulatory authority or licensee after the implementation of financial crime control measures.
Risk Profile	The risk profile of an institution is determined on the basis of two main dimensions, the ML/TF risk level and the ML/TF control level. Factors for the inherent risk score are geographic scope, the customer base of the institution, the products and services and the distribution channel of the institution. For the control level, the governance and control procedures of an institution, the adequacy of the compliance function, the compliance history and incidents and the quality of preventative measures in the institution are relevant factors. (***FATF Guidance for a Risk-Based Approach***).
Layering	This is the second stage in money laundering. Layering refers to the use of funds, which originate from criminal conduct, to perform various financial transactions, which serve the dual purpose of concealing the illegal originating source of the funds, and to distance

the funds from this source with the intention that the funds will appear to be legitimate.

Annex I – Financial Crime Risk Factors

The December 2015 – February 2016 Edition of *ACAMS Today*, gives a comprehensive analysis of financial crime risk factors or red flags, as follows:

"COUNTRY RISK

The overall reputation of a country should be factored into the risk model. For example, certain countries or jurisdictions have high levels of corruption or unstable governments. Some are known as

Bank secrecy and ML havens or suffer from high levels of drug production and shipping, and cartel activities. Information sources to help identify reputational risk include: Transparency International's

Corruption Perceptions Index and the U.S. State Department's annual International Narcotics Control Strategy Report (INCSR), which rates countries based on their ML controls and corruption. It is important to establish a documented geography risk rating methodology that leverages internal and external information sources, including at least a review of sanctions and TF lists published by governments and international organizations such as those published by the U.S. Office of Foreign Assets Control

(OFAC), the U.K. Financial Conduct Authority (FCA), the U.N. Security Council Committee, the U.S. Financial Crimes Enforcement Network (Fin CEN) and the EU.

The risk model may take into account whether a country is a member of the Financial Action Task Force (FATF) or of an FATF-style regional body, and has implemented practices in line with

international standards set out by the FATF and other international organizations.

The risk model should also take into account regional risks inside a particular country, such as the cross-border areas between nations, or designated areas of high intensity financial crime or drug trafficking, such as the U.S. High Intensity Financial Crime Areas or High Intensity Drug Trafficking Areas.

SECTOR RISK

Some sector risks—regarding corruption and bribery, in particular—might include the following:

- *Sectors which are strongly influenced by government or state owned entities*
- *Public sector procurement and government contracts*
- *Sectors which are not subject to regulation*
- *Sectors in which corrupt practices are endemic*

According to the OECD Foreign Bribery Report (2014), those sectors most exposed to corrupt practices include the following:

- *Commodities sector*
- *Real estate*
- *Transport*
- *Information and communication*

Sectors particularly vulnerable to ML include the above, but in particular they include the financial services sectors and companies trading in consumer goods.

CUSTOMER RISK

The following includes a list of red flags attached to customers. Beyond those listed below, any indirect risks which emerge through association or other issues which are of reputational concern and which undermine the integrity of the customer should be identified. It is useful to consult other red flag check lists included in FATF reports, the Good Practice Guidelines on Conducting Third Party Due Diligence (published by the World Economic Forum in 2013), or other sources like Australia's FIU, which has published some 70 red flag indicators.

- *Foreign financial institutions*
- *Targets of financial sanctions*
- *Non-bank financial institutions*
- *Non-transparent beneficial ownership*
- *Contradictory information*
- *Politically exposed persons (PEPs)*
- *Third-party relationships*
- *Offshore structures*
- *Shell companies or shelf companies*

PRODUCT/TRANSACTION RISK

Common product and transaction risks include the following whereby each product will in turn have its own red flags:

- *Wealth management*
- *Trusts and foundations*
- *Relationship to correspondent banks*
- *Mobile payments*
- *Value transfer through virtual worlds and digital currencies*
- *Payable through accounts and concentration accounts*
- *Life insurance and annuities*

Red flags for trade-based finance might include the following:

- *Private banking and correspondent banking*
- *Payments to vendors in cash by unrelated third parties*
- *Payments to vendors by wire transfers from unrelated third parties*
- *Payments to vendors by checks, bank drafts or postal money orders from unrelated third parties*
- *False reporting, such as commodity misclassification, overvaluation or under-valuation*
- *Carousel transactions, meaning repeated importation and exportation of the same high-value commodity*
- *Trading in commodities that do not match the business*
- *Unusual shipping routes or trans-shipment points*
- *Packaging that is inconsistent with the commodity or shipping method*
- *Double-invoicing"*

Examples of Controls

Licensees should take into account the following control factors to mitigate the above risks (which are not set up in any particular order of importance nor should they be considered exhaustive:

a) Assessment and Understanding the Risk facing an institution;
b) Proper governance arrangements;
c) An effective three lines of defense regime;
d) Implementing an adequate transaction monitoring system;
e) Effective CDD policies in regards to Customer Acceptance Policy, Customer and Beneficial Owner Identification, Verification and Risk Profiling;
f) Procedures and Policies for Ongoing Monitoring of its Customer's activities and Risk Profile;
g) Management of Information, which includes; Record Keeping and Updating of Information;
h) Reporting of Suspicious Transactions and Asset Freezing;
i) Group-wide Information Sharing and Cross Border Considerations (subsidiaries and branches of an institution should have policies and procedures which are aligned with Head Office); and
j) Effective Outsourcing Policies (which includes Attestations)

Annex II – Control Functions & Typologies

CONTROL FUNCTIONS

Group of Financial Sector Regulators

Supervisory coordination is undertaken through the Group of Financial Services Regulators ("GFSR") which includes as members all three principal prudential supervisors. Other participants in these meetings include representatives from the Department of Cooperatives, Compliance Commission ("CCB"), the Financial Intelligence Unit ("FIU") and the Office of the Attorney General ("OAG"). Members are signatories to the Memorandum of Understanding (MoU) allowing information sharing as needed to effectively supervise the financial institutions and designated non-financial businesses and professionals. The MoU includes information sharing provisions for effective oversight of the financial and non-financial sectors and arrangements for consolidated supervision of the single conglomerate/group in The Bahamas, including but not limited to, regular communication, monitoring of capital and intergroup transactions and some mutual decision-making regarding supervisory approvals and reprimand

TYPOLOGIES

- FLORENCE, Italy, Feb 17 (Reuters) - Bank of China (BOC) agreed to pay a 600,000 euro fine to settle a money laundering case involving its Milan branch, court documents seen by Reuters showed. The Florence court hearing the case gave four employees of the Milan branch of China's fourth biggest bank a suspended two-year prison sentence for failing to report illicit money transfers. Florence prosecutors leading the so-called "River of Money" investigation alleged that more than 4.5 billion euros ($4.78 billion) was smuggled to China from Italy between 2006 and 2010 by Chinese people living mainly in Florence and nearby Prato. About half of the money was sent via BOC, the prosecutors said. The court also ordered BOC to pay back 980,000 euros which it said it had earned through the illegal operations. According to the prosecutors, the proceeds sent to China came from a series of illegal activities, including counterfeiting, embezzlement, exploitation of illegal labor and tax evasion.

- The biggest trial in Cayman Islands history, a multibillion-dollar fraud case investigating the collapse of a Saudi business empire. The economic impact of the trial for Cayman's legal and financial services sector is likely to be substantial. It alleges that Maan Al Sanea, who married into the family and managed its financial services businesses, engaged in massive unauthorized borrowing, siphoning off proceeds to his own companies, many of them registered in the Cayman Islands, and triggering the collapse of the entire business empire. (Cayman Compass, July 2017)

- A man who laundered tens of thousands of dollars for drug dealers has been jailed. Cordell Simmons, 59, wired nearly USD 80,000 worth of ill-gotten gains to accounts in Jamaica and the U.S. so that criminals abroad could collect the cash. Simmons was paid

around USD100 for every USD1,000 he wired abroad by drug dealers who wanted to get the "dirty money" out of Bermuda. He made dozens of transfers for amounts of up to $3,000 at a time through Western Union and MoneyGram between June 2008 and November 2009. Yesterday Simmons was jailed for two years. (Bermuda Sun, June 2010)

A former Credit Suisse Group AG wealth manager was found guilty of orchestrating a scheme that resulted in damages of 143 million Swiss francs ($152 million) as he diverted cash from client accounts to cover bad trades in one of the biggest financial crimes in Swiss history. After two weeks of deliberations, Patrice Lescaudron, who catered to wealthy eastern Europeans, was sentenced to five years in prison by a judge in Geneva.. Despite the banker's claims that he never profited from his illicit trades, the judge found that the 54-year-old gained 30 million francs from his deception.