

GUIDANCE NOTE

GUIDANCE NOTE ON THE PREVENTION OF MONEY LAUNDERING, COUNTERING THE FINANCING OF TERRORISM AND COUNTERING PROLIFERATION FINANCING

Including the Treatment of Politically Exposed Persons

PUBLISHED DATE: OCTOBER 2026

Securities Commission of The Bahamas

All rights reserved. No part of this publication may be reproduced or distributed without the prior written permission of the publisher.
This document does not constitute legal advice.

This publication is available at www.scb.gov.bs.

© Copyright 2026 Securities Commission of The Bahamas

GUIDANCE NOTE ON THE PREVENTION OF MONEY LAUNDERING, COUNTERING THE FINANCING OF TERRORISM AND COUNTERING PROLIFERATION FINANCING

Including the Treatment of Politically Exposed Persons

For all Licensees and Registrants of the Securities Commission of The Bahamas

TABLE OF CONTENTS

PART A: INTRODUCTION AND FRAMEWORK	5
1. Introduction.....	5
2. Purpose and Status of this Guidance.....	5
3. Applicability.....	6
4. Legislative and Regulatory Framework	7
5. Demonstrating Effectiveness: the FATF Immediate Outcomes.....	7
PART B: THE RISK-BASED APPROACH	9
6. Overview of the Risk-Based Approach	9
7. The Self-Risk Assessment	9
8. The Customer Risk Rating Framework	10
9. New Products, Practices and Technologies	11
PART C: GOVERNANCE AND INTERNAL CONTROLS	12
10. Board and Senior Management Responsibility.....	12
11. The Compliance Officer and the Money Laundering Reporting Officer	12
12. Independent Testing	13
13. Outsourcing and Reliance on Third Parties	13
14. Group-Wide Programmes and Employee Integrity.....	14
PART D: CUSTOMER DUE DILIGENCE	15
15. Core CDD Obligations	15
16. Timing, Failure to Complete, and Exemptions	15
17. Simplified Due Diligence	16
18. Enhanced Due Diligence.....	17
19. Ongoing Monitoring and Periodic Review	18
PART E: POLITICALLY EXPOSED PERSONS.....	19

20. Purpose and Principles of the PEP Regime	19
21. Definitions and Categories	19
22. Identifying PEPs: Risk Management Systems and Screening	20
23. Risk Rating PEPs	21
24. Enhanced Due Diligence and Ongoing Measures for PEPs	23
25. PEP Declassification	24
PART F: TERRORIST FINANCING, PROLIFERATION FINANCING AND TARGETED FINANCIAL SANCTIONS	26
26. Terrorist Financing	26
27. Targeted Financial Sanctions: Obligations Without Delay	26
28. Proliferation Financing: Understanding the Risk	27
29. PF Risk Indicators	28
PART G: SECTOR-SPECIFIC GUIDANCE	30
30. Securities and Capital Markets (SIA Registrants)	30
31. Investment Funds and Fund Administrators (IFA Regulated Persons)	30
32. Financial and Corporate Service Providers (FCSPA Licensees)	31
33. Digital Asset Businesses and Registered Exchanges (DARE Registrants)	32
PART H: SUSPICIOUS TRANSACTION REPORTING, RECORDS AND TRAINING	35
34. Suspicious Transaction Reporting	35
35. Record Keeping	35
36. Education and Training	36
PART I: SUPERVISION, EFFECTIVENESS AND ENFORCEMENT	37
37. The Commission's Supervisory Approach	37
38. Enforcement	37
39. Interpretation and Review of this Guidance	37
APPENDIX A: APPLICABILITY MATRIX	39
APPENDIX B: ILLUSTRATIVE LIST OF BAHAMIAN DOMESTIC PEPs	40
APPENDIX C: PEP DECLASSIFICATION CHECKLIST	41
APPENDIX D: CONSOLIDATED PF RED-FLAG INDICATORS	42
APPENDIX E: REFERENCE MATERIALS	44
APPENDIX F: GLOSSARY OF ABBREVIATIONS	45

PART A: INTRODUCTION AND FRAMEWORK

1. Introduction

1. The Securities Commission of The Bahamas (the "Commission") issues this Guidance Note on the Prevention of Money Laundering, Countering the Financing of Terrorism and Countering Proliferation Financing, including the Treatment of Politically Exposed Persons (the "Guidance Note" or "this Guidance"), for all licensees and registrants under the Commission's regulatory remit (collectively, "regulated persons").
2. Money laundering ("ML"), terrorist financing ("TF") and proliferation financing ("PF") threaten the integrity, stability and reputation of The Bahamas' capital markets and financial services sector. The Commission expects every regulated person, through its board of directors and senior management, to embed the prevention, detection and reporting of ML, TF and PF within its enterprise risk management strategy, proportionate to the nature, size and complexity of its business.
3. This Guidance consolidates and expands upon the Commission's supervisory expectations under the sector-level anti-money laundering, countering the financing of terrorism and countering proliferation financing ("AML/CFT/CPF") Rules administered by the Commission, and reflects the standards of the Financial Action Task Force ("FATF"), the International Organization of Securities Commissions ("IOSCO"), and comparative supervisory practice internationally.
4. The Guidance is deliberately practical. It explains not only what the law and the Rules require, but how the Commission expects regulated persons to demonstrate that their controls work in practice, that is, to demonstrate effectiveness in the sense contemplated by the FATF's Immediate Outcomes. Throughout this document, boxed "Commission's Expectations" summarise the practical evidence the Commission will look for during supervision.

2. Purpose and Status of this Guidance

5. The purpose of this Guidance Note is to: (a) assist regulated persons in understanding and discharging their statutory and regulatory AML/CFT/CPF obligations; (b) set out the Commission's supervisory expectations for effective, risk-based implementation of those obligations; (c) provide comprehensive, risk-based guidance on the identification, risk rating, treatment, monitoring and declassification of politically exposed persons ("PEPs"); (d) support consistency of practice across the securities, investment funds, financial and corporate services, and digital asset sectors; and (e) strengthen the effectiveness of The Bahamas' national AML/CFT/CPF regime, including in the context of the Caribbean Financial Action Task Force ("CFATF") mutual evaluation process.
6. This Guidance does not constitute legal advice and does not replace or override the provisions of any Act, Regulation or Rule. Where any conflict arises between this Guidance and legislation or Rules, the legislation or Rules prevail. However, the Commission will have regard to this Guidance when assessing whether a regulated person has complied with its obligations, and a failure to

follow this Guidance without a documented, reasoned alternative approach that achieves an equivalent or better outcome may be taken into account in supervisory and enforcement action. The applicable Rules themselves require regulated persons, when developing AML/CFT/CPF policies and procedures, to pay due regard to guidelines, best practices and policy statements issued by the Commission.

7. The word "must" is used in this Guidance where an obligation arises under legislation or Rules. The words "should" or "is expected to" indicate the Commission's supervisory expectation of how compliance is ordinarily achieved; a regulated person departing from such an expectation should be able to demonstrate to the Commission how its alternative approach achieves the underlying objective.

3. Applicability

8. This Guidance Note apply to all persons licensed or registered by the Commission under the following legislation (each together with its subsidiary legislation):
- the Securities Industry Act, 2024 (No. 39 of 2024) ("SIA"), including registered firms and registrable securities business;
 - the Investment Funds Act, 2019 ("IFA"), including licensed investment funds and investment fund administrators;
 - the Financial and Corporate Service Providers Act, 2020 ("FCSPA"), including financial and corporate service providers acting as designated non-financial businesses and professions ("DNFBPs") and trust and company service providers ("TCSPs"); and
 - the Digital Assets and Registered Exchanges Act, 2024 (No. 40 of 2024) ("DARE"), including digital asset businesses and registered exchanges.
9. The sector-level AML/CFT/CPF Rules applicable to each category of regulated person are: (a) the Securities Industry (Anti-Money Laundering, Countering the Financing of Terrorism and Countering Financing of Proliferation) Rules, 2026, which revoke and replace the 2015 Rules (the "SIA AML Rules"); (b) the Investment Funds (Anti-Money Laundering, Countering the Financing of Terrorism and Countering the Financing of Proliferation) Rules, 2026 (the "IFA AML Rules"); (c) the Financial and Corporate Service Providers (Anti-Money Laundering, Countering the Financing of Terrorism and Countering Financing of Proliferation) Rules, 2026, which revoke and replace the 2019 Rules (the "FCSP AML Rules"); and (d) the Digital Assets and Registered Exchanges (Anti-Money Laundering, Countering the Financing of Terrorism and Countering Financing of Proliferation) Rules, 2026, which revoke and replace the 2022 Rules (the "DARE AML Rules"). Each set of 2026 Rules was gazetted on 27 October 2026. A consolidated applicability matrix is set out at Appendix A.
10. The four sets of Rules are deliberately tailored to the risks and business models of their respective sectors; differences between them reflect sector-specific calibration, not inconsistency. A regulated person holding licences or registrations under more than one Act must comply with each set of Rules applicable to the activities conducted under the relevant licence or registration;

where a single customer relationship or transaction engages activities under more than one licence, the applicable requirements apply cumulatively.

11. This Guidance should be read together with the Group of Financial Services Regulators ("GFSR") Guidelines on Countering Proliferation Financing (2025) and any guidance issued by the Identified Risk Framework ("IRF") Steering Committee, the Financial Intelligence Unit ("FIU") and the Office of the Attorney-General.

4. Legislative and Regulatory Framework

12. The principal national legislation comprising The Bahamas' AML/CFT/CPF framework includes: the Financial Transactions Reporting Act, 2018 ("FTRA") and the Financial Transactions Reporting Regulations, 2018; the Financial Transactions Reporting (Wire Transfers) Regulations, 2018; the Proceeds of Crime Act, 2018 ("POCA"); the Anti-Terrorism Act, 2018 ("ATA"), including section 9 (financing of proliferation of weapons of mass destruction) and the framework for implementing United Nations Security Council Resolutions ("UNSCRs"); the International Obligations (Economic and Ancillary Measures) Act (Ch. 16), under which targeted financial sanctions are imposed; the Financial Intelligence Unit Act; and the sector Acts and Rules identified in section 3 above.
13. The 2026 Rules adopt the concept of "identified risks": references to money laundering, the financing of terrorism and the financing of proliferation, where used in relation to the assessment, management or mitigation of risk, are construed under the Rules to include all identified risks as defined under the FTRA, within the identified risk framework established under the POCA. References in this Guidance to "identified risks" carry the same meaning. Regulated persons should ensure that their policies, procedures, training materials and monitoring scenarios reflect this broader framing and are not confined to a narrow, offence-by-offence reading.
14. The Bahamas' framework gives effect to the FATF Recommendations. Of particular relevance to this Guidance are: Recommendation 1 (assessing risks and applying a risk-based approach, including PF risk assessment); Recommendations 9–23 (preventive measures, including Recommendation 10 on customer due diligence, Recommendation 12 on PEPs, Recommendation 15 on new technologies and virtual assets, Recommendation 16 on payment transparency, and Recommendation 22 on DNFBPs); Recommendations 6 and 7 (targeted financial sanctions relating to terrorism and to proliferation); and Recommendations 24 and 25 (beneficial ownership).

5. Demonstrating Effectiveness: the FATF Immediate Outcomes

15. International assessments of The Bahamas measure not only technical compliance with the FATF Recommendations but the effectiveness of the regime in practice, expressed through the FATF Immediate Outcomes ("IOs"). Regulated persons contribute most directly to: IO.3 (supervisors appropriately supervise, monitor and regulate financial institutions and virtual asset service providers, and those institutions adequately apply AML/CFT preventive measures commensurate with their risks and report suspicious transactions); IO.4 (the corresponding outcome in respect of designated non-financial businesses and professions, including financial and corporate service

providers); IO.10 and IO.11 (terrorists, and persons and entities involved in the proliferation of weapons of mass destruction, are prevented from raising, moving and using funds, including through the implementation of targeted financial sanctions without delay); and IO.1 (risks are identified, assessed and understood, and actions coordinated domestically).

- 16.** In practical terms, effectiveness means that a regulated person can show, with records, data and worked examples, that its controls actually operate and actually change outcomes. The Commission distinguishes between the existence of a policy and the demonstration of a control. During examinations and thematic reviews, the Commission will test both.

Commission's Expectations: Evidencing Effectiveness

- Board and senior management can articulate the firm's ML/TF/PF risks in their own words and evidence challenge (minutes, management information, approvals and escalations).
- The SRA demonstrably drives the control environment: risk ratings map to due diligence depth, monitoring intensity, review cycles and resourcing.
- Screening, monitoring and reporting systems produce auditable outputs: alert volumes, disposition rationales, quality assurance sampling, and timeliness metrics.
- Suspicious transaction reporting is prompt, well-reasoned and of usable quality; internal reports that are not escalated carry a documented rationale by the MLRO.
- Targeted financial sanctions obligations are executed without delay, with evidenced screening at onboarding, on list updates and on trigger events, and with test records.
- Remediation of examination findings and internal audit findings is tracked to closure with dates, owners and evidence.

- 17.** The Commission engages with industry on an ongoing basis (through consultation on rules where undertaken, outreach sessions, thematic feedback, and published examination observations) and expects regulated persons to engage constructively in return, including by attending industry briefings, completing surveys and declarations within stipulated timelines, and raising interpretive questions with the Commission early rather than after the fact.

PART B: THE RISK-BASED APPROACH

6. Overview of the Risk-Based Approach

18. The risk-based approach ("RBA") is the foundation of the AML/CFT/CPF regime. It requires a regulated person to identify, assess and understand the ML, TF and PF risks to which it is exposed, and to apply resources and mitigating measures commensurate with those risks: enhanced measures where risks are higher; simplified measures, where permitted and approved, where risks are lower. An RBA is not a zero-failure regime, and it does not permit a regulated person to avoid its obligations; it provides disciplined flexibility in how obligations are met.
19. A blanket approach, treating all customers, products or jurisdictions as posing identical risk, is inconsistent with the RBA and is itself a supervisory concern, because it typically produces both over-compliance that indiscriminately restricts legitimate access to financial services (including de-risking of entire customer classes) and under-compliance in the areas of genuinely elevated risk.

7. The Self-Risk Assessment

20. Every regulated person must conduct and document an enterprise-wide assessment of its ML/TF/PF risks, being its Self-Risk Assessment ("SRA"), the Commission's term for what the FATF describes as the business or business-wide risk assessment, consistent with sections 5 and 14 of the FTRA and the risk rating framework duty in the applicable sector Rules. This section should be read together with the Commission's Guidance Note on Self-Risk Assessments and its sector annexes, which set out the Commission's detailed expectations and prevail on matters of SRA methodology and review. The assessment must cover, at a minimum: (a) customers and beneficial owners, including customer types and concentrations; (b) countries and geographic areas in which the regulated person operates or with which its customers and transactions are connected; (c) products, services and transactions, including their inherent vulnerability to abuse; (d) delivery channels, including non-face-to-face onboarding and intermediated or introduced business; and (e) for digital asset businesses, technological factors including supported assets, protocols and counterparty exposure.
21. The SRA should follow a structured methodology: identify and assess inherent risk; establish risk tolerance approved by the board; establish mitigation measures (controls); evaluate residual risk against tolerance; and monitor and review. The methodology, data inputs, scoring logic and conclusions should be documented in sufficient detail that a knowledgeable third party, including a Commission examiner, can reperform the assessment and reach the same conclusions.
22. The SRA must be kept current. Section 5(2) of the FTRA requires a risk assessment to be carried out prior to the launch of a new product or business practice, prior to the use of new or developing technologies, and upon a major event or development in the management and operations of the group. In addition to these statutory triggers, the Commission expects review at least annually, and upon: entry into a new market or client segment; a material change in ownership,

management or business model; a material finding by the Commission, an auditor or the regulated person's own compliance function; publication of a new or revised National Risk Assessment ("NRA") or relevant sectoral assessment; and relevant FATF, CFATF or IRF Steering Committee findings. Each review and each pre-launch assessment must be evidenced and documented in writing (section 5(3)), even where the conclusion is that no change is required.

- 23.** The SRA must incorporate proliferation financing risk as a distinct dimension, consistent with FATF Recommendation 1 and the GFSR CPF Guidelines. PF risk is addressed in detail in Part F of this Guidance; for the purposes of the SRA, a regulated person should assess its exposure to breach, non-implementation and evasion of PF-related targeted financial sanctions, having regard to its customer base, trade and payment corridors, dual-use goods exposure, and (for digital asset businesses) exposure to sanctioned or high-risk on-chain counterparties.

Commission's Expectations: Self-Risk Assessment

- A current, dated, board-approved SRA exists, with a documented methodology and an accountable owner identified by post.
- The SRA uses the firm's own data (customer counts by risk tier and type, PEP population, jurisdictional exposure, product volumes, alert and STR statistics), not generic sector narrative alone.
- ML, TF and PF are separately assessed; TF and PF are assessed with the same rigour and specificity as ML.
- The residual risk conclusions visibly drive the compliance monitoring plan, training plan, and resourcing decisions for the following period.
- Trigger-based refreshes (new products, technologies, group events) are evidenced, not merely provided for on paper.

8. The Customer Risk Rating Framework

- 24.** Each regulated person must implement a customer risk rating framework which assigns a risk rating to every customer at onboarding and keeps that rating current throughout the relationship. The framework should combine, with documented weightings or logic: customer risk factors (legal form and transparency of ownership; occupation or industry; PEP status; sanctions or adverse information exposure; behaviour during onboarding); geographic risk factors (residence, nationality, place of incorporation and operation; connections to high-risk or monitored jurisdictions, including those identified by the FATF, by the IRF Steering Committee, or in the NRA); product and service risk factors (complexity, liquidity, cross-border reach, anonymity features, ability to receive third-party payments); and delivery channel risk factors (non-face-to-face onboarding, introduced or intermediated business, reliance on third parties).
- 25.** Risk ratings should use at least three tiers (for example low, medium, high), with defined consequences for each tier: the depth of due diligence, the level of approval required, the frequency of periodic review, and the intensity of transaction monitoring. Overrides of model-generated ratings (in either direction) must be documented, reasoned and approved at an appropriate level.

- 26.** A customer's risk rating is dynamic. Events that should prompt reassessment include: a customer becoming a PEP; material adverse information; unusual or unexplained activity; changes to ownership, control or business profile; connections emerging to high-risk jurisdictions; sanctions list changes; and the periodic review cycle. The Rules require that due diligence be periodically reviewed and kept up to date on the basis of materiality and risk, at appropriate times, taking into account the adequacy of data previously obtained, and, where the applicable Rules prescribe minimum review or re-verification intervals, those intervals must be observed: in every sector, higher risk relationships must be reviewed at least annually, and the intervals for other risk tiers are those prescribed by the applicable Rules. The Commission expects reviews toward the earlier end of any prescribed range, in every case upon trigger events, and immediately, with enhanced due diligence, upon suspicion of any identified risk.

9. New Products, Practices and Technologies

- 27.** Before launching a new product, service, business practice or delivery mechanism, or deploying a new or developing technology (including artificial intelligence tools used in onboarding, screening or monitoring), a regulated person must assess and document the ML/TF/PF risks that may arise and implement appropriate mitigating measures before launch. For digital asset businesses this includes the listing or support of a new digital asset, protocol, or transfer mechanism, and any material change to custody or wallet infrastructure.
- 28.** Where automated tools or models materially influence AML/CFT/CPF decisions (screening disposition, risk scoring, transaction monitoring), the regulated person remains fully responsible for outcomes, must understand the tool's logic and limitations, must validate and periodically test performance (including false negative testing), and must retain the ability to explain individual decisions to the Commission.

PART C: GOVERNANCE AND INTERNAL CONTROLS

10. Board and Senior Management Responsibility

- 29.** Ultimate responsibility for AML/CFT/CPF compliance rests with the board of directors (or equivalent governing body) and senior management of the regulated person. The board must: approve the Self-Risk Assessment, the risk tolerance, and the AML/CFT/CPF policies and procedures; ensure that adequate resources, systems and expertise are in place; receive and challenge regular management information on the operation of the control framework; and satisfy itself that deficiencies are remediated. Outsourcing, reliance on third parties, group arrangements or technology failures do not relieve the board or senior management of these duties.
- 30.** Management information presented to the board or a designated committee should, at a minimum and at least quarterly for higher-risk businesses, cover: customer population by risk tier; PEP and sanctions-exposed relationships; onboarding rejections and exits for financial crime reasons; screening and monitoring alert volumes, ageing and disposition; internal reports and STRs filed; overdue periodic reviews; training completion; audit and examination findings and remediation status; and material regulatory developments.

11. The Compliance Officer and the Money Laundering Reporting Officer

- 31.** Every regulated person must appoint a Compliance Officer ("CO") and a Money Laundering Reporting Officer ("MLRO") and register those appointments with the Commission (and, for the MLRO, with the FIU as applicable). The roles may be combined only where proportionate to the nature, size and complexity of the business and where no conflict impairs the effectiveness of either function.
- 32.** The MLRO must have sufficient seniority, independence and authority: unfettered access to customer files, transaction records and systems; direct access to the board or a board committee; and freedom from business-line influence over the assessment of internal reports. The MLRO is responsible for receiving and assessing internal suspicion reports, determining whether an STR must be made, overseeing prompt filing, and maintaining complete records of reports received, determinations made and the reasons for them, including reasoned decisions not to file.
- 33.** The CO is responsible for the day-to-day operation and maintenance of the AML/CFT/CPF programme: keeping policies and procedures current; operating or overseeing screening and monitoring; running the training programme; conducting compliance monitoring and testing; and serving as the principal point of contact with the Commission. Vacancies in either post must be notified to the Commission promptly, with interim arrangements documented; obligations are attached to the post and continue notwithstanding any vacancy.

12. Independent Testing

- 34.** The AML/CFT/CPF programme must be subject to periodic independent testing, by internal audit or a competent external party, on a cycle commensurate with risk (at least every two years, and annually for higher-risk businesses). Testing should be substantive (sample-based reperformance of due diligence, screening, monitoring and reporting controls), not limited to policy review. Findings must be reported to the board or audit committee and tracked to remediation.

13. Outsourcing and Reliance on Third Parties

- 35.** A regulated person may outsource operational, technical or compliance functions, but retains ultimate legal responsibility and liability for compliance. Before entering into a material outsourcing arrangement, the regulated person must conduct and document due diligence on the provider, covering technical capability, reliability and resilience; cybersecurity; regulatory status and the AML/CFT/CPF standards of the jurisdictions in which the provider operates or stores data; financial stability, reputation and ownership; and conflicts or concentration risks, and must refresh that assessment at least annually or upon material change.
- 36.** Outsourcing contracts for regulated functions should secure, in writing (and, for digital asset registrants, must address the matters specified in the outsourcing policy published by the Commission, including): immediate and unrestricted access to customer due diligence records, transaction logs, analytics outputs and audit trails; audit and inspection rights for the regulated person, its auditors and the Commission; data protection and encryption obligations; prior written consent for sub-outsourcing of core components; and notification within 24 hours of any cybersecurity breach, system failure or regulatory non-compliance affecting the outsourced function. Digital asset registrants are additionally subject to the specific requirements of the DARE AML Rules concerning third-party technology providers: documented due diligence before any arrangement for critical or regulated functions, review of that due diligence at least annually or upon material change, and compliance with the outsourcing policy published by the Commission, which addresses written contractual protections, access and audit rights, prior notification to the Commission of material arrangements, breach notification, business continuity and documented exit strategies. The Commission may also object to the appointment or continued use of an outsourced Money Laundering Reporting Officer, in which case the appointment must be terminated promptly.
- 37.** Reliance on the customer due diligence of another financial institution is permitted only within the strict limits of the applicable Rules, which vary by sector: the third party must be a regulated entity subject to AML/CFT/CPF obligations and supervision, must not be located in a listed high-risk country, and must provide written confirmation of verification and confirm the existence of the relevant account or facility. Copies of identification data and underlying verification documents must be available from the third party without delay upon request by the regulated person or the Commission. Reliance never transfers responsibility: if the third party's due diligence proves deficient, the regulated person remains accountable.

- 38.** Eligible introducer arrangements must comply with the applicable Rules, including the obligation to terminate the relationship where required information and documentation is not received from the introducer within thirty days of the introducer's confirmation. Introduced business should be treated as a distinct delivery-channel risk factor in the customer risk rating framework, and the regulated person should periodically test samples of introduced files against the introducer's confirmations.

14. Group-Wide Programmes and Employee Integrity

- 39.** A regulated person that is part of a group should implement group-wide AML/CFT/CPF programmes, including policies for sharing information required for CDD and risk management, with adequate safeguards on confidentiality and use. Where the minimum requirements of a host jurisdiction of a branch or subsidiary are lower than those of The Bahamas, the Bahamian standard should be applied to the extent permitted; where local law prevents this, the regulated person must apply appropriate additional measures and inform the Commission.
- 40.** Screening procedures must ensure high standards of probity when hiring employees, and periodically thereafter for staff in sensitive roles. Employees' own accounts and dealings should be subject to monitoring appropriate to their role. Performance incentives should never reward conduct that undermines AML/CFT/CPF controls.

PART D: CUSTOMER DUE DILIGENCE

15. Core CDD Obligations

41. A regulated person must not establish a business relationship or execute an occasional transaction without applying customer due diligence measures to identify and verify the identity of the customer and of any beneficial owner, using independent and reliable source documents, data or information (whether or not electronically sourced). CDD must also establish the ownership and control structure of legal persons and arrangements, the purpose and intended nature of the business relationship, and, commensurate with risk, the source of funds and, where appropriate, the source of wealth.
42. For natural persons, verification should cover full legal name and any aliases, date of birth, nationality, and government-issued photographic identification, together with at least two current means of contact in accordance with the applicable Rules (which may include personal or business email address, telephone numbers, and mailing, business or residential addresses including the elements specified in the Rules). Documents may be accepted as originals; as certified copies where originals are impractical; or as photographed or scanned copies where the regulated person has adequate, internationally recognised tools to verify authenticity.
43. For legal persons and legal arrangements, CDD must identify: proof of incorporation or registration and legal form; the registered office and principal place of business; directors, officers, partners, trustees, founders or council members as applicable; the constitutional documents and authority of persons acting; and every beneficial owner, that is, each natural person who ultimately owns or controls the customer (applying the ownership threshold in the applicable framework) and, where no natural person is identified through ownership, the natural persons exercising control through other means, and failing that the senior managing official. Complex, multi-layered or cross-border structures with no evident commercial rationale are a recognised indicator of elevated risk and call for enhanced measures, including diagramming the structure to the ultimate natural persons and understanding why each layer exists.
44. Particular care is required for trusts, foundations, executive entities, investment condominiums, segregated accounts companies, partnerships, non-profit associations and nominee or omnibus arrangements. For trusts, the settlor, trustee(s), protector (if any), beneficiaries or classes of beneficiaries, and any other natural person exercising ultimate effective control must be identified. For nominee shareholders and directors, the nominator must be identified. For omnibus and intermediated arrangements, see paragraph 20.5 and Part G.

16. Timing, Failure to Complete, and Exemptions

45. Verification of identity must be completed before establishing the business relationship or executing the occasional transaction, save only in the narrow circumstances permitted by the applicable framework where verification may be completed as soon as reasonably practicable after establishment, where this is essential not to interrupt the normal conduct of business and

ML/TF/PF risks are effectively managed through documented interim controls (such as transaction restrictions and prohibition on outward transfers).

- 46. Where CDD cannot be completed, the regulated person must not open the account, commence the business relationship or perform the transaction; must suspend activity where reasonable direct verification efforts have failed; must terminate the relationship where the Rules so require; and must consider whether an STR is warranted. Exiting a customer for CDD failure never displaces the reporting obligation, and the manner of exit must not amount to tipping off.
- 47. The applicable Rules permit specified categories of customer to be treated as presenting lower risk (for example, financial institutions and digital asset businesses licensed or registered by the Central Bank, the Commission, the Insurance Commission, the Compliance Commission or the Gaming Board; foreign institutions subject to and supervised for AML/CFT/CPF obligations consistent with the FATF Recommendations, with adequate CDD and record-keeping procedures; central or local government agencies or statutory bodies; and publicly traded companies listed on registered or specified markets with adequate transparency of beneficial ownership), and simplified due diligence may be applied to them in accordance with section 17, alongside any exemption available under the FTRA framework. This treatment does not relieve the regulated person of risk assessment, sanctions screening, ongoing monitoring or reporting obligations, and it must not be applied where there is any suspicion of identified risks.

17. Simplified Due Diligence

- 48. A regulated person may apply simplified due diligence ("SDD") measures to a customer, business relationship or transaction only where: (a) it has assessed the associated ML/TF/PF risk as low in accordance with its risk rating framework, consistent with any risk assessment carried out at the national level and any guidance issued by the Commission; (b) there is no suspicion of ML, TF or PF; and (c) no higher-risk circumstance of the kind identified in the applicable Rules or under section 13 of the FTRA applies. The basis for the lower-risk determination, and the SDD measures applied, must be documented. SDD means adjusting the extent, timing or type of measures, not dispensing with CDD.
- 49. Acceptable simplification may include: reduced frequency of periodic identity refresh; reduced volume of corroborating documentation; or inferring purpose and intended nature from the product itself. Sanctions and PEP screening, ongoing monitoring, and record-keeping are never simplified away. The Commission may direct a regulated person not to apply, or to cease applying, SDD measures, and any such direction must be complied with. A regulated person must itself monitor for indicators that a customer no longer qualifies, and must cease applying SDD and revert to the measures otherwise required where it knows or suspects ML, TF or PF or where the risk is no longer low.

18. Enhanced Due Diligence

- 50.** Enhanced due diligence ("EDD") must be applied to categories of customers, business relationships or transactions presenting higher risk. Without limitation, higher risk indicators under the Rules and this Guidance include a customer who: is from or established in, or is a party to a transaction connected with, a country identified by the IRF Steering Committee or otherwise assessed as higher risk; presents complexity of ownership or legal structure with no apparent commercial justification; conducts transactions inconsistent in size, frequency or pattern with the customer's profile or known source of funds or wealth; is unable to produce required KYC information and documentation; uses anonymous, randomly generated or temporary email services; persistently structures activity to avoid KYC or reporting thresholds; or is a politically exposed person. Transactions may present higher risk where, for example, they are peer-to-peer, involve unusual complexity or size, break an audit trail, or involve cross-border elements which reduce the regulated person's ability to apply effective oversight and controls.
- 51.** EDD measures under the Rules include, as appropriate to the risk: corroborating identity against third-party databases or other reliable sources; for non-face-to-face verification, video conferencing, notarised or equivalently certified documentation, and verification of additional identity elements or biometric data held electronically; tracing the customer's IP address; corroborating activity against the customer's transaction profile; obtaining additional information on source of funds and source of wealth; obtaining information on the reasons for intended or performed transactions; enhanced monitoring of the relationship and transactions; and requesting transaction and trading history. Under the FCSP and IFA AML Rules, enhanced due diligence must include obtaining additional information on the customer and beneficial owner, establishing source of funds and source of wealth, obtaining senior management approval before establishing or continuing the relationship, and enhanced ongoing monitoring. In every sector, the measures selected should be recorded, together with the rationale connecting them to the specific risks identified.
- 52.** High-risk countries. Regulated persons must apply EDD proportionate to the risks arising from business relationships and transactions connected with countries identified by the FATF as High-Risk Jurisdictions subject to a Call for Action or Jurisdictions under Increased Monitoring, countries identified by the IRF Steering Committee or in the NRA, and countries the regulated person itself assesses as higher risk (having regard to corruption perception, sanctions exposure, terrorism and proliferation concerns, and the strength of AML/CFT/CPF supervision). Where the FATF calls for countermeasures, the regulated person must apply them. Caution should also be exercised over certified documentation originating from high-risk countries, with enhanced verification of its legitimacy.
- 53.** Non-face-to-face business. Non-face-to-face onboarding is a standing feature of the securities, funds and digital asset sectors and is not inherently unacceptable, but it must be treated as a delivery-channel risk factor and mitigated through robust identity-proofing: reliable digital identity systems with appropriate assurance levels; liveness detection and document authenticity tooling; and the EDD measures listed above where risk warrants.

19. Ongoing Monitoring and Periodic Review

54. After verification is concluded and the relationship established, the regulated person must: monitor the conduct of the relationship on an ongoing basis; ensure that activity remains consistent with the customer's risk profile, expected activity and source of funds; scrutinise transactions that are complex, unusually large, conducted in unusual patterns, or have no apparent economic or lawful purpose; and keep CDD information current on the basis of materiality and risk, taking into account the adequacy of data previously obtained. Monitoring calibration (rules, scenarios, thresholds) should reflect the SRA and be periodically tuned and tested, with tuning decisions documented.
55. Where an investor or customer is introduced through an intermediary, nominee or omnibus platform, the regulated person must assess whether it has timely access to underlying investor and beneficial ownership information, apply EDD, and ensure that such information is available in accordance with the applicable Rules. Inability to obtain look-through information commensurate with risk should lead to refusal or exit of the arrangement.
56. Previous business relationships. Where a relationship was terminated and the customer later returns, the regulated person should not simply reactivate historic CDD: it must confirm identity data remains current, refresh screening, and consider the reasons for the earlier termination, particularly where the customer was exited for financial crime reasons, in which case re-onboarding should require senior management approval and documented justification.

PART E: POLITICALLY EXPOSED PERSONS

20. Purpose and Principles of the PEP Regime

57. Individuals entrusted with prominent public functions may be in a position to abuse their office and influence for personal gain through bribery, corruption or other illicit conduct, and the proceeds of such conduct heighten the ML/TF/PF risks to which financial services businesses are exposed. The close relationships between PEPs and their family members and close associates can create additional channels for illicit activity. The FTRA, the sector Rules and FATF Recommendations 12 and 22 therefore require additional measures for PEPs.
58. Two principles frame this Part. First, PEP measures are preventive, not punitive: the majority of PEPs neither abuse nor are in a position to abuse their functions, and refusing a relationship solely because a person is a PEP is contrary to the letter and spirit of Recommendation 12 and to the Commission's expectations on financial inclusion. Second, PEP risk is not uniform: the level of risk varies significantly with the function held, the level of influence, access to or control over public funds and decisions, the jurisdiction concerned, and time in and out of office. A blanket approach that treats every PEP as posing the same corruption risk is inconsistent with the risk-based approach.
59. This Part is designed to ensure that PEPs receive consistent treatment across the Bahamian financial sector, while tailoring expectations to the Commission's regulated sectors and their Rules.

21. Definitions and Categories

60. Under the FTRA and the sector Rules, a "politically exposed person" means an individual who is or has been entrusted with: (a) a prominent public function within The Bahamas (a "domestic PEP"), inclusive of a head of state or government, senior politician or legislator, senior government, judicial or military official, senior executive of a state-owned corporation, or an important political party official; (b) a prominent public function by a foreign jurisdiction (a "foreign PEP"), inclusive of the equivalent roles; or (c) a prominent function within an international organisation (an "international organisation PEP"), including directors, deputy directors, members of the board, members of senior management, or individuals entrusted with equivalent functions. "International organisation" means an entity established by a formal political agreement equivalent in status to an international treaty, made between, and recognised by law in, member countries, and not treated as a resident institutional unit of the country in which it is located, for example the United Nations, the International Monetary Fund, the Organization of American States, the Inter-American Development Bank and comparable regional bodies.
61. The regime extends to: family members, being individuals related to a PEP directly or through marriage or a similar form of partnership, including a spouse or partner, parent, child or sibling; close associates, being natural persons closely connected to a PEP socially or professionally,

including any person in a position to conduct substantial domestic or international financial transactions on behalf of the PEP; and any corporation, business or other entity formed by or for the benefit of a PEP. "Prominent public function" does not extend to middle-ranking or more junior officials, though seniority of title is not determinative; the substance of the function, and in particular influence over public funds, procurement, licensing and appointments, is what matters.

- 62. Under the DARE AML Rules, PEP procedures and controls must additionally address relationships with any legal person in which a PEP is a director, officer, founder or council member; a partner or trustee; a signatory or a person authorised to undertake transactions; a holder of a beneficial interest of ten per cent or more; a person with principal control over the legal person's assets; or a person exercising control over its management. These connections are broader than beneficial ownership alone, and the Commission expects every regulated person, whatever its sector, to design screening and onboarding processes capable of detecting each of them, including PEPs appearing as authorised signatories or trading authorities on accounts they do not own.
- 63. An illustrative (non-exhaustive) list of Bahamian domestic PEP categories (including all individuals required to file financial disclosures with the Public Disclosure Commission under the Public Disclosure Act, 1976 and the 1980 Notice) is set out at Appendix B. Where a role does not appear on the list, the regulated person must apply a principles-based assessment of whether the function is prominent and classify accordingly, documenting its reasoning.

22. Identifying PEPs: Risk Management Systems and Screening

- 64. Section 41 of the FTRA requires appropriate risk management systems to determine whether a facility holder or beneficial owner is politically exposed, and the sector Rules require clear procedures and controls for identifying and verifying PEPs both at establishment of the relationship and where an existing customer becomes a PEP. Identification must therefore operate at onboarding and continuously thereafter.
- 65. A multi-source approach is required; no single source is sufficient. Sources should include: (a) structured customer self-declaration at onboarding covering the customer's own status and known family and associate connections, with periodic re-confirmation; (b) screening of customers, beneficial owners, controllers, directors, trustees and authorised signatories against commercial PEP databases and reliable public sources, at onboarding, on database updates, and on trigger events; (c) domestic sources, including the Appendix B categories, official gazettes, parliamentary and senate registers, and announcements of public appointments; (d) adverse media screening; and (e) intelligence arising from the relationship itself, such as transaction counterparties, powers of attorney and references in correspondence.
- 66. Screening effectiveness expectations. Fuzzy matching must be calibrated to the naming conventions relevant to the customer base, and calibration decisions (thresholds, exclusion rules) documented and tested, including periodic seeded false-negative testing. Alert dispositions must record the reviewer (by post), the date, the rationale, and the evidence relied upon. Wholesale

discounting of alerts, template rationales, and disposition backlogs are recurring supervisory findings internationally and will be treated as indicators of an ineffective control.

- 67.** Because commercial databases have imperfect coverage of domestic and regional figures, regulated persons should not rely on database screening alone for Bahamian and regional PEP identification, and should maintain awareness of local public life through the domestic sources described above. Conversely, database inclusion is not conclusive of PEP status: the regulated person must form and document its own view against the statutory definition.

23. Risk Rating PEPs

- 68.** Once identified, every PEP relationship must be risk rated. The central question is whether the individual's current or previous politically connected role gives rise to a material probability of increasing the regulated person's exposure to ML, TF or PF. Ratings should be at least three-tier (lower, intermediate, high) and must be individually reasoned: the classification "PEP" is the trigger for assessment, not the conclusion of it.
- 69.** Foreign PEPs, and their family members and close associates, are always treated as high risk, and the full suite of EDD measures in section 24 must be applied. There is no discretion to rate a foreign PEP relationship as lower risk, although the intensity of measures within the high-risk band may still be calibrated to the specific facts.
- 70.** Domestic PEPs and international organisation PEPs, and their family members and close associates, may be rated across the risk spectrum on the basis of a documented assessment. The assessment must consider, at a minimum: the individual's seniority and level of influence; access to or control of public funds, procurement, licensing, appointments or other decisions of value; the nature of the products or services sought and whether funding sources are verifiable and traceable to low-risk sources such as employment income or publicly documented investments; the terms of the relationship and whether it facilitates ordinary personal or routine commercial activity; the individual's personal source of funds and wealth relative to observed financial flows; length of time in office and in the specific portfolio; and jurisdictional corruption risk. The assessment of a lower-risk rating must be robust without being unreasonably onerous, and must build in review triggers to detect material change in the PEP's status or transacting pattern.
- 71.** Indicators supporting a lower risk rating for a domestic or international organisation PEP include:

Indicator	Description
Easily verifiable identity	Identity of the PEP, family members and close associates is readily confirmed through reliable sources, including full legal name and aliases, date of birth, nationality and authentic government-issued identification.
Low-risk products and services	The products or services sought are assessed as low risk for criminal exploitation, based on the verified originating source and, where applicable, the terminal use of funds, for example a facility receiving verifiable salary income connected to the appointed or elected position.

Indicator	Description
Limited decision-making power	The public position carries no significant executive decision-making authority or material influence over financial decisions connected with positions of trust (public contracts, employment, licences).
Low-risk country of origin	The relevant country is associated with minimal corruption and criminal activity, by reference to credible indices such as the Transparency International Corruption Perceptions Index.
Transparent business relationship	The nature and purpose of the proposed relationship are easily understood and commercially coherent.
Verifiable source of wealth	Source of funds and wealth is readily verifiable and proportionate to the products or services requested, for example salaried income or earnings on verifiable assets.

- 72.** Family members and close associates of a lower-risk domestic PEP may themselves ordinarily be treated as lower risk, unless review of any indicator triggers suspicion requiring additional scrutiny; the obligation to monitor transactions through the accounts effectively remains in all cases.
- 73.** Indicators requiring a high risk rating for a domestic PEP (in addition to the mandatory high rating of all foreign PEPs) include:

Indicator	Description
Wealth earned from government connections	Assessed potential for significant wealth or financial flows derived from government licences, monopolies, preferential access to privatised assets, or contracts in sectors with limited competition or high barriers to entry created by law, regulation or policy.
Inconsistent financial flows or wealth	Incongruence between verifiable sources of wealth and observed financial flows, or lifestyle inconsistent with known legitimate income.
Allegations of misconduct	Credible accusations of financial crimes or misconduct, or ongoing or past investigations, suggesting heightened likelihood of involvement in corrupt activities.
Questionable appointments	Appointment to public office disproportionate to the individual's qualifications or merits, or indicative of nepotism, raising concern about abuse of power for personal gain.
High-risk sector or portfolio	Influence over defence and procurement, extractive industries, major construction and public works, gaming, state-owned enterprises, or other sectors known to carry elevated corruption exposure.

- 74.** Special consideration must be given to family members and close associates of high-risk domestic PEPs, assessing whether their income, wealth or financial flows derive from: granting of government licences or contracts; licences to act as a monopoly provider or permissions for significant construction projects; preferential access to the privatisation of former crown assets;

commerce in sectors with high barriers to entry or limited competition, especially where those barriers stem from law, regulation or government policy; wealth or lifestyle inconsistent with known legitimate sources; or appointments to public office inconsistent with personal merit or professional experience.

24. Enhanced Due Diligence and Ongoing Measures for PEPs

- 75.** For every PEP relationship, in addition to normal CDD, the regulated person must, using a risk-based approach: (a) deploy appropriate risk management systems to determine whether the customer or beneficial owner is a PEP; (b) maintain clear policy, internal guidelines, procedures and controls governing such relationships; (c) obtain senior management approval before commencing the relationship, and before continuing a relationship with a customer found to be or who becomes a PEP; (d) take reasonable measures to establish the source of wealth and source of funds of the customer and beneficial owner; and (e) conduct enhanced ongoing monitoring of the relationship and its transactions so that changes are detected and assessed for unusual or suspicious character. Under the sector Rules, measures (c) to (e) are mandatory in every case for a foreign PEP, whether as customer or beneficial owner, and must also be applied to a domestic or international organisation PEP wherever the relationship presents a higher risk; the requirements apply, with the necessary changes, to family members, close associates and entities formed by or for the benefit of a PEP.
- 76.** For lower-risk PEPs, proportionate EDD may comprise: additional information verifying the non-suspicious nature of transactions from reliable independent sources; source of funds checks confirming funds are not linked to suspicious activity; understanding of the purpose and nature of the relationship; identification and verification of the ultimate beneficial owner of transaction proceeds, including control structures; and ongoing monitoring for unusual activity or behavioural change, with periodic review at the standard cycle for the assigned tier.
- 77.** For high-risk PEPs, rigorous oversight is required, including: enhanced wealth verification (independent verification of source of wealth using public records and financial disclosures, not solely self-reported explanations, with the economic activity that created the wealth documented); active senior management approval and oversight supported by a detailed risk assessment and written justification; review and approval by the risk management committee (or equivalent governance forum) to ensure robust challenge; shorter review cycles (at least annually, and more frequently on trigger); deeper periodic reviews covering transactions, behaviour and changes in role or circumstances; enhanced transaction monitoring using tailored scenarios and, where available, advanced analytics; and close scrutiny of complex structures, unusual features (very large transactions, use of government or central bank accounts, particular demands for secrecy, cash or instruments that break an audit trail, unknown financial institutions, and regular transactions just below reporting thresholds).
- 78.** A profile of expected activity should be developed for each PEP relationship at onboarding, used as the baseline for monitoring, and regularly reviewed and updated. Where proposed or existing PEP relationships give grounds for suspicion, timely reports must be made to the FIU; the fact of

PEP status must never delay a report. Regulated persons should also remain alert to the risk that existing customers acquire PEP connections after onboarding (through marriage, appointment or association) and ensure trigger and periodic review processes capture this.

- 79.** Beneficiaries of investment products. Where a product or arrangement provides for payment or transfer of value to a designated beneficiary other than the customer (including designated beneficiaries of fund interests, custody or investment accounts, and transfers on death or assignment), the regulated person must take reasonable measures to determine whether the beneficiary, or any beneficial owner of the beneficiary, is a politically exposed person, at the latest at the time of payout, redemption or transfer of the value concerned. Where a PEP is identified and higher risks are present, the regulated person must inform senior management before the payout or transfer proceeds, conduct enhanced scrutiny of the whole relationship, and consider whether a suspicious transaction report is warranted. Under the IFA AML Rules, enhanced due diligence is mandatory in every case where subscription monies are received from, or redemption proceeds are to be paid to, a person other than the investor.
- 80.** Decisions to decline or exit PEP relationships should be documented with the same rigour as decisions to accept them. If risks are understood and properly addressed, acceptance of a PEP is a legitimate business decision like any other; conversely, indiscriminate refusal of PEPs, particularly domestic PEPs performing ordinary personal banking-equivalent activity in the securities and funds sectors, may indicate an ineffective risk-based approach.

25. PEP Declassification

- 81.** Declassification (the removal of PEP designation and associated measures from an individual who no longer holds a prominent public function) must follow a risk-based, case-by-case assessment, not a fixed timetable alone. Factors to be assessed include: linkage to high-risk industries (including financial and quasi-financial services, virtual asset service providers, casinos and gaming, real estate and property development, DNFBPs, precious metals and high-value goods, arms and dual-use trade, cash-intensive businesses, and cross-border trade and shipping); position-specific risks, including the sphere of influence of the function previously held; tenure in office; the likelihood of re-entering public life, considering public activity, financial capacity and continuing political connections; source of wealth, particularly wealth acquired while in office; the plausibility of the individual's risk profile and declared net worth; and any negative media concerning the individual's financial affairs. For former foreign PEPs, the corruption risk of the country concerned must additionally be evaluated.
- 82.** Minimum period. A domestic PEP who ceases to hold the prominent public function must remain subject to risk-based enhanced due diligence for no less than twenty-four months after ceasing to hold the function. Continuation beyond that minimum is dictated by the individual's risk profile against the factors above; the influence of some figures, for example former Prime Ministers or long-serving ministers with enduring party or commercial networks, can extend well beyond tenure, and such cases should not be declassified merely because the minimum period has elapsed.

- 83.** Governance. Declassification of any PEP, family member or close associate requires review and approval by senior management, with the assessment and approval documented and retained. Prior PEP status must remain visible on the customer record for future investigative purposes, including potential STR filings. For deceased PEPs, the position must be documented; where the relationship continues with surviving family members or close associates, a risk-based assessment must determine whether continued EDD or declassification is appropriate. Declassification should be integrated into ongoing monitoring (through risk-based assessment, consistent monitoring, reporting, notices and the express removal of the designation) rather than occurring by silent lapse.

Commission's Expectations: PEP Framework

- A documented PEP policy covering identification, connection tests for legal persons, risk rating with reasoned tiering, EDD by tier, approval authorities (by post), monitoring, periodic review, declassification and record-keeping.
- A complete and current PEP register: every PEP, family member and close associate relationship, its category (domestic/foreign/international organisation), rating, approval, source of wealth and funds evidence, expected activity profile, last review and next review dates.
- Evidence that senior management approvals are substantive: the approver saw the risk assessment and the source of wealth analysis, and the approval predates account activity.
- Screening calibration, testing and disposition records as described in section 22, including domestic-source coverage of Bahamian public life.
- Declassification files showing the case-by-case assessment, the 24-month minimum observed for domestic PEPs, senior management approval, and retention of prior status.
- Management information to the board on the PEP population, new approvals, exits and overdue reviews.

PART F: TERRORIST FINANCING, PROLIFERATION FINANCING AND TARGETED FINANCIAL SANCTIONS

26. Terrorist Financing

- 84.** Terrorist financing differs from money laundering in a critical respect: the funds involved may be of entirely legitimate origin, and the amounts involved may be small. Detection therefore depends less on tracing criminal proceeds and more on recognising patterns, such as the destination and purpose of funds, connections to persons or organisations of concern, and behaviours inconsistent with the customer's profile. Regulated persons must ensure their risk assessments, monitoring scenarios and training treat TF as a distinct risk, having regard to the ATA, the NRA, and typologies published by the FATF, CFATF and the FIU. The FATF's Comprehensive Update on Terrorist Financing Risks (2025) finds that terrorist financiers increasingly combine conventional techniques (cash couriers, hawala and other money or value transfer services) with digital channels, including online payment services, social media and crowdfunding features, gaming platforms and virtual assets; that decentralised structures, regional financial hubs, self-financed cells and lone actors drawing small sums from legitimate income and petty crime are increasingly prominent and harder to detect; that ethnically, racially or politically motivated terrorism presents low-visibility financial footprints, compounded by inconsistent designations across jurisdictions; and that terrorist financing increasingly converges with organised crime. Regulated persons should reflect these trends in their risk assessments, indicator sets, monitoring scenarios and training.
- 85.** Particular vigilance is warranted in relation to: non-profit associations and charities identified as at risk of abuse; transfers to or from conflict zones or jurisdictions identified for TF concern; crowdfunding and rapid pass-through of small sums across many counterparties; and, in the digital asset sector, the use of privacy-enhancing technologies or unhosted wallets to obscure the destination of value.

27. Targeted Financial Sanctions: Obligations Without Delay

- 86.** The Rules embed targeted financial sanctions ("TFS") obligations directly in each sector's AML/CFT/CPF Rules. Every regulated person must establish and maintain policies, procedures, systems and controls to ensure compliance with TFS pursuant to section 3A of the International Obligations (Economic and Ancillary Measures) Act and section 44 of the ATA, and must: (a) freeze, without delay and without notice to the designated person or entity, funds or other assets of designated persons and entities, including assets owned or controlled by them (wholly or jointly, directly or indirectly), assets derived or generated from such assets, and assets of persons acting on behalf of or at the direction of a designated person or entity; and (b) inform the Attorney-General and the FIU that it holds such funds or assets, providing details. For digital asset registrants, funds and other assets expressly include digital assets. A regulated person must also cooperate with any legal action for the forfeiture or confiscation of frozen assets, and must not

make any funds available, directly or indirectly, to or for the benefit of a designated person or entity.

87. "Without delay" is to be construed strictly: action within hours, not days, of designation or discovery. Regulated persons must maintain the capability to screen their entire customer and counterparty population against updated lists immediately upon promulgation, to freeze at once, and to report at once. The Commission disseminates UNSCR designation notices and declarations received through national channels; regulated persons must action and return declarations within the stipulated timelines, must disclose on the declaration any matches to existing customers or business relationships, and must immediately sever prohibited relationships in accordance with the applicable directions.
88. An effective sanctions screening framework comprises, at a minimum: a sanctions risk assessment; appropriate policies and procedures; internal controls, including list management ensuring all applicable UN lists (and any additional lists to which the regulated person is exposed by virtue of its business, currencies or group membership) are captured and updated automatically; educated and experienced employees; and adequate testing, including periodic seeded-name testing of screening systems. The board and senior management are responsible for approving and overseeing the framework, ensuring adequate resources, systems and expertise, setting the sanctions risk appetite, and ensuring policies are implemented, monitored and updated in line with legislative and regulatory requirements.
89. Screening must occur: at onboarding, before any transaction is executed; upon every list update, across the full customer base including beneficial owners, controllers, directors and authorised signatories; in real time on payments and transfers, including wire transfer payer and payee information under the Financial Transactions Reporting (Wire Transfers) Regulations; and on trigger events. Name-matching calibration, exclusion logic and disposition standards follow the same effectiveness expectations set out for PEP screening in Part E. Attempted transactions involving designated parties, and any freeze actions, should also be assessed for STR filing.

28. Proliferation Financing: Understanding the Risk

90. Proliferation financing is the provision of funds or financial services 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, contrary to section 9 of the ATA and applicable UNSCRs. In the FATF framework, PF risk is assessed principally as the risk of breach, non-implementation or evasion of the PF-related TFS obligations (currently relating to the Democratic People's Republic of Korea and Iran, the United Nations measures in respect of Iran having been reinstated in September 2025 under the snapback mechanism).
91. PF differs from ML and TF in ways that matter for control design: funds are frequently legitimate in origin (state or corporate); the activity is trade-centred, involving dual-use goods (items with both civilian and military applications) and complex logistics; and the actors are typically

sophisticated networks using front and shell companies, falsified documentation, ship-to-ship transfers, and intermediaries in third countries to evade controls. PF risk therefore concentrates in trade finance, cross-border payments, corporate structures with opaque ownership, and, increasingly, virtual assets used to evade the traditional financial system.

- 92.** Every regulated person must include PF risk as a distinct dimension of its Self-Risk Assessment (see Part B): identifying how its customers, products, corridors and channels could be used to breach or evade PF-related TFS; assessing likelihood and impact; and implementing commensurate mitigation. Regulated persons should consult the GFSR Guidelines on Countering Proliferation Financing (2025), including its sectoral guidance for Commission registrants and licensees, and the FATF Guidance on Proliferation Financing Risk Assessment and Mitigation. Regulated persons should also have regard to the FATF's report on Complex Proliferation Financing and Sanctions Evasion Schemes (2025), which identifies four principal evasion typologies: the use of intermediaries, including front and shell companies and third-country brokers; the obscuring of beneficial ownership to gain access to the financial system; the use of virtual assets and related technologies to generate and move value, including large-scale thefts from virtual asset businesses and the earnings of overseas information technology workers; and the exploitation of the maritime and shipping sectors, including deceptive shipping practices. The report identifies the Democratic People's Republic of Korea as the most significant proliferation financing actor, combining growing financial connectivity with diversified revenue.

29. PF Risk Indicators

- 93.** The presence of a single indicator does not itself warrant suspicion, but should trigger further monitoring; the presence of multiple indicators calls for thorough examination and consideration of reporting. Indicators drawn from the FATF and GFSR guidance include the following (a fuller compilation appears at Appendix D):
- 94.** Customer profile indicators: vague or incomplete information about proposed trading activities at onboarding and reluctance to elaborate when queried; the customer or its owners or senior managers appearing in sanctions lists, negative news, or past or ongoing investigations; connections to a country of proliferation concern; dealing in dual-use goods, export-controlled goods, or complex equipment for which the customer lacks technical background or which is incongruent with its stated activity; previous violations of export control regimes; participation in complex trade deals with numerous third-party intermediaries in lines of business differing from the onboarding profile; a commercial business transacting like a money-remittance or pay-through operation, with rapid, high-volume movement and small end-of-day balances without clear rationale; affiliation with a university or research institution combined with dual-use goods trading; and the desire to use cash for industrial or trade transactions.
- 95.** Account and transaction indicators: transactions by or to persons ordinarily resident or domiciled in a country of proliferation or diversion concern; transactions involving items controlled under dual-use or export control regimes; involvement of companies with non-transparent ownership, front companies or shell companies; long dormancy followed by a surge of activity; counterparties

exchanging goods that share owners, management, physical address, IP address or telephone number, or otherwise coordinating; circuitous transaction routing; involvement of financial institutions in countries with weak UNSCR implementation or export control regimes; sudden influxes of cash deposits followed by withdrawals; ledger arrangements structured to avoid frequent international financial transactions; and personal accounts used to purchase industrial or export-controlled items.

96. Trade finance indicators: requests for letters of credit for dual-use or export-controlled shipments prior to account approval; inconsistencies between trade documents and financial flows (names, addresses, final destination); a freight forwarder listed as a product's final destination; and wire instructions or payments to or from entities not identified on the original documentation.
97. For digital asset businesses, additional PF evasion indicators include: exposure (direct or within a risk-appropriate hop limit) to wallet clusters attributed to designated persons, state-sponsored cyber actors or ransomware campaigns; use of mixers, privacy pools or chain-hopping consistent with sanctions evasion; Travel Rule information conflicting with on-chain attribution; exposure to wallet clusters attributed to thefts or hacks of virtual asset businesses by state-sponsored actors; and payment flows consistent with the earnings of undisclosed overseas information technology workers. These are addressed further in Part G.

Commission's Expectations: TFS and CPF

- Documented evidence of screening at onboarding, on every list update, and in payment flows, with timestamps demonstrating action without delay.
- A PF dimension in the Self-Risk Assessment, proportionate to the firm's actual trade, corridor and (for digital asset businesses) on-chain exposure.
- Completed UNSCR declarations returned within stipulated timelines, with any matches disclosed and relationships severed as directed.
- Records of freezes effected, reports made to the Attorney-General and the FIU, and notifications to designated parties.
- Periodic testing of screening systems, including seeded-name and list-update latency testing, with results reported to senior management.
- Training content and monitoring scenarios that address PF and dual-use goods specifically, not generically.

PART G: SECTOR-SPECIFIC GUIDANCE

30. Securities and Capital Markets (SIA Registrants)

98. The securities sector's vulnerabilities differ from deposit-taking: the sector can be abused not only to launder proceeds generated elsewhere (placement is often already achieved through the banking system) but also to generate illicit proceeds within the sector itself, through market manipulation, insider dealing, boiler-room and recovery-room fraud, unauthorised trading and misappropriation. Layering is the stage most visible to securities firms: rapid movement between accounts, products and jurisdictions; churning without economic rationale; and conversion between cash equivalents and securities. Regulated persons should draw on the FATF Report on ML/TF in the Securities Sector and the securities-sector risk-based approach guidance in designing scenarios.
99. Indicators warranting scrutiny in this sector include: funding of accounts from unrelated third parties, or requests to pay redemption or sale proceeds to third parties or to accounts in different names or jurisdictions than the funding source; deposits of physical securities or bearer instruments; transactions that make no investment sense (buying and selling at a loss with rapid withdrawal; wash-like patterns; indifference to fees or performance); use of the account as a pass-through with minimal investment activity; trading in illiquid or low-priced securities susceptible to manipulation; structuring below thresholds; and sudden activity inconsistent with the customer's profile. The Rules specifically require mitigation of additional risks arising from the cross-border nature of transactions, particularly where a transaction takes place in a jurisdiction which could reduce the regulated person's oversight and the application of effective AML/CFT/CPF controls: regulated persons should map their cross-border flows and apply commensurate controls, including corridor-specific monitoring.

31. Investment Funds and Fund Administrators (IFA Regulated Persons)

100. The IFA AML Rules, 2026 establish a complete AML/CFT/CPF framework for investment funds, their operators, licensed and foreign investment fund administrators and investment fund managers. Responsibility for compliance rests with the investment fund itself, and its operators must ensure that the fund complies. Functions may be delegated, including to the fund's administrator, under a written delegation agreement, but the fund and its operators remain responsible for the performance of every delegated function. Each fund must maintain a written compliance programme proportionate to its nature, size, complexity, structure and risk profile, and must appoint a fund Compliance Officer and a fund Money Laundering Reporting Officer with the prior written approval of the Commission. An investment fund manager is not required to establish a separate compliance programme in respect of the fund; its obligations under the Rules include performing any delegated investment-side functions, reporting knowledge or suspicion without delay, and keeping records and producing them within five business days of a request. A fund licensed at the commencement of the Rules has twelve months to establish its compliance programme and risk assessment and to make the required appointments.

- 101.** The dominant sectoral risk is intermediated distribution. Where an investor subscribes as a nominee or intermediary for underlying investors, the Rules require the fund to identify and verify those underlying investors, unless the nominee or intermediary is an eligible introducer, has been assessed as presenting a risk no higher than standard, and has undertaken in writing to provide the identification information and records of the underlying investors within five business days of a request. A master fund may treat each feeder fund that invests in it as its investor on the conditions the Rules specify. Reliance on an eligible introducer never transfers responsibility: the required identity information and written confirmation of verification must be obtained before a subscription is accepted, copies of the identification documents must follow within thirty days, and where they do not, the fund must verify the investor directly or suspend the relationship and, where verification cannot be completed, terminate it. In practice this means due diligence on the intermediary itself (regulatory status, supervision, programme quality, jurisdiction), periodic testing of its ability to deliver underlying investor data on request, and refusal or exit where look-through commensurate with risk cannot be achieved.
- 102.** Subscription and redemption controls are prescribed: subscription monies may be accepted, and redemption proceeds and distributions paid, only through an account held in the name of the investor with an institution regulated for AML/CFT/CPF purposes in The Bahamas or in a country that is not a high-risk jurisdiction, unless enhanced due diligence has been applied; cash is prohibited in both directions; and enhanced due diligence is mandatory where subscription monies are received from, or redemption proceeds are to be paid to, a person other than the investor, and for any subscription, redemption or transfer that is complex, unusually large or without apparent economic or lawful purpose. Fund-specific indicators warranting scrutiny include rapid subscription and redemption inconsistent with the fund's strategy or notice periods (using the fund as a pass-through); frequent transfers of holdings between apparently unrelated parties; investors indifferent to redemption penalties, gates or fees; funding inconsistent with the investor's known profile; and in-specie subscriptions of assets of uncertain provenance. On the investment side, the Rules require risk-based due diligence on counterparties and investee entities, screening of those persons against the lists of designated persons or entities before transacting and without delay upon list updates, and enhanced measures for higher-risk investments, including private companies, real property, digital assets and assets connected with high-risk jurisdictions; investment-side functions may be delegated only with the prior written approval of the Commission. Administrators should ensure registrar and transfer-agency monitoring covers these patterns, and the Rules fix investor review intervals (at least annually for higher risk, and not exceeding three years for standard risk and five years for low risk investors).

32. Financial and Corporate Service Providers (FCSPA Licensees)

- 103.** FCSPs (including those acting as company formation agents, registered agents and registered offices, providers of directors, officers and nominee shareholders, and related trust and corporate services) occupy the gateway through which legal persons and arrangements enter the financial system, and are therefore central to FATF Recommendations 22, 24 and 25. Misuse of corporate vehicles (shell companies, layered cross-jurisdictional chains, nominee arrangements concealing

beneficial ownership, and dormant entities reactivated for transactions) is a recurring feature of ML, sanctions evasion and PF typologies worldwide.

- 104.** Licensees must therefore: identify and verify the beneficial owner of every entity formed or administered, and keep that information accurate and current; understand and document the purpose of each structure and the commercial rationale for each layer; decline structures whose evident purpose is concealment; where providing nominee services, identify the nominator and record the nominee status; and monitor for changes in ownership, control, directors and activity, including sudden changes shortly after formation. Particular vigilance is required around: requests for aged or shelf companies; instructions from professional intermediaries who resist disclosing the client; entities with bearer-instrument history; entities whose declared activity involves dual-use goods, shipping, trade intermediation or high-value goods; and PEP connections at any level of a structure, which engage the connection tests described in Part E.
- 105.** Because FCSP services are frequently the first Bahamian touchpoint for foreign principals, licensees should assume that the quality of their CDD determines the quality of information available to every downstream institution and authority, and should calibrate their evidential standards accordingly, including for the identified risk framework and beneficial ownership registry obligations applicable under Bahamian law.

33. Digital Asset Businesses and Registered Exchanges (DARE Registrants)

- 106.** The DARE AML Rules, 2026 impose the most technologically specific obligations in the Commission's framework, reflecting FATF Recommendation 15 and its Interpretive Note. A registrant's risk rating framework must identify and mitigate the risks arising from products, services or activities provided to or by anonymous or private sources, including unhosted wallets, the darknet and blacklisted addresses, particularly where the risk rating is high or where the type, size and volume of transactions is substantial, and must address the customer, product, channel and cross-border risk factors prescribed by the Rules, including the types of digital assets supported.
- 107.** Ongoing monitoring. Monitoring under the Rules includes scrutiny of transactions throughout the relationship (including, where necessary, source of funds) against the registrant's knowledge of the customer, their business and risk profile; keeping due diligence information current; analysing blockchain and similar transactions on a risk basis, taking into account the nature of the registrant's business; and, where large volumes of transactions occur on a regular basis, the use of automated monitoring systems, provided that flagged transactions are subject to human expert analysis to determine whether they are suspicious. The Commission expects monitoring to operate across all supported ledgers and protocols, to correlate on-chain activity with off-chain customer profile data, and to be supported by documented analytics providers, attribution methodology and alerting thresholds, with provider coverage validated for the assets supported.
- 108.** Higher-risk indicators. The Rules identify digital asset specific circumstances in which enhanced due diligence must be applied, including: involvement in mining operations in high-risk

jurisdictions or involving higher-risk digital assets; digital assets with anonymity-enhancing features, or products and services that obfuscate transactions or undermine the registrant's ability to know its customers; requested exchanges to or from cash, or to or from state-sponsored digital assets suspected of being used to avoid sanctions; digital assets that come from, or are associated with, the darknet, unregulated exchanges, market abuse, ransomware, hacking, fraud, Ponzi schemes or sanctioned digital asset addresses; peer-to-peer transactions; and the results of blockchain or similar analysis indicating higher risk.

- 109.** Transfers of digital assets. The Rules apply the wire transfer framework to every transfer of digital assets, giving effect to the FATF Travel Rule through the Financial Transactions Reporting (Wire Transfers) Regulations: an ordering registrant must obtain and hold required and accurate originator and beneficiary information, submit it to the counterparty institution immediately and securely, and must not execute a transfer where it cannot do so; an intermediary must retain the information with the transfer and identify transfers lacking it; and a beneficiary registrant must obtain and hold the required information, verify the identity of the beneficiary where not previously verified, identify transfers lacking required information, and apply risk-based policies for determining when to execute, reject or suspend a deficient transfer and the appropriate follow-up action. The information must be made available promptly to the Commission, the FIU and any other authority lawfully entitled to request it. Before submitting information to a counterparty institution, a registrant must take reasonable measures to identify the counterparty and determine whether it is subject to AML/CFT/CPF obligations and can reasonably be expected to protect the confidentiality of the information; the outcome of those measures informs whether to execute, reject or suspend the transfer.
- 110.** Unhosted wallets. Where a transfer of digital assets is made to, or received from, an unhosted wallet, the registrant must obtain the required originator and beneficiary information from its customer and assess the transfer in accordance with its risk rating framework; where a higher risk is presented, it must apply mitigation commensurate with that risk, which may include the enhanced due diligence measures described above, limits on such transfers, or enhanced monitoring. The Commission expects registrants to maintain the capability to distinguish transfers with regulated counterparty institutions from transfers involving unhosted wallets, to screen wallet addresses against sanctions-related and other blacklisted address data, and to refuse or suspend transfers whose risks cannot be effectively mitigated. Where monitoring or analysis gives rise to suspicion, the registrant must report in accordance with Part H.
- 111.** Records and technology governance. Comprehensive records of monitoring, blockchain analysis, alerts and investigation files must be maintained in accordance with Part H. The outsourcing regime summarised in Part C applies with particular force to transfer messaging providers, blockchain analytics vendors, customer due diligence utilities and wallet custody infrastructure: the Rules require documented due diligence before any arrangement for critical or regulated functions, review at least annually or upon material change, and compliance with the outsourcing policy published by the Commission, which addresses contractual protections, access and audit

rights, prior notification of material arrangements, breach notification, business continuity and exit strategies.

Commission's Expectations: Digital Asset Registrants

- Demonstrable, tested capability to distinguish transfers with counterparty institutions from transfers involving unhosted wallets, with the decision logic documented.
- Blockchain analytics coverage validated for every supported asset and chain; uncovered assets treated as a risk acceptance requiring senior management sign-off.
- Alert-to-investigation-to-report workflow evidenced end to end, with human expert analysis of flagged transactions and timestamps demonstrating prompt escalation and reporting.
- Counterparty institution assessments conducted before transfer information is submitted, reviewed and kept current.
- Vendor files for analytics, messaging, customer due diligence and custody providers meeting the Rules and the outsourcing policy published by the Commission, with prior notification of material arrangements.
- Board-level reporting on on-chain exposure, including sanctions-exposed volume and exposure to anonymity-enhancing services.

PART H: SUSPICIOUS TRANSACTION REPORTING, RECORDS AND TRAINING

34. Suspicious Transaction Reporting

- 112.** Every regulated person must implement policies and procedures enabling any employee to report knowledge or suspicion that a customer is or may be engaged in activities associated with identified risks to the MLRO, and the MLRO must assess the sufficiency of each internal report. Where there are reasonable grounds for suspicion, including in relation to attempted transactions and proposed relationships, an STR must be filed with the FIU promptly. The Rules expressly emphasise promptness; regulated persons should set and monitor internal service standards for the time from alert to internal report, internal report to MLRO determination, and determination to filing.
- 113.** Suspicion is a lower threshold than proof: it requires a degree of satisfaction, beyond mere speculation, that is at least founded on observed facts, such as activity inconsistent with the profile, unexplained sources, structuring, refusal to provide information, or the presence of the indicators described throughout this Guidance. Quality matters as much as timeliness: reports should clearly identify the parties, accounts and transactions concerned, state the grounds for suspicion in plain terms, and attach or reference supporting material, so that the FIU can act on them. Defensive filing of unreasoned reports undermines the effectiveness of the reporting regime and is itself a supervisory concern.
- 114.** Tipping off. No person may disclose to the customer or any third party that an STR or related information has been or may be filed, or that an investigation is contemplated or under way, where the disclosure is likely to prejudice it. Exit and freeze communications must be crafted accordingly, and staff trained on permissible wording. Records of internal reports, MLRO determinations (including reasoned non-filings) and STRs must be maintained securely with strictly limited access.

35. Record Keeping

- 115.** Records of customer identity, business relationships and transactions must be maintained for at least seven years from the later of the date the customer ceases to be a facility holder or the completion of the transaction, and records relating to ongoing investigations or STRs for such longer period as required. Records must be sufficient to enable: competent third parties to assess the regulated person's observance of its AML/CFT/CPF policies and procedures; individual transactions to be reconstructed (including amounts, currencies and counterparties); the regulated person to respond fully and rapidly to court orders and enquiries from the Commission and other competent authorities; and customers to be identified. Records may be kept in any retrievable format, provided integrity, security, and prompt availability are assured, including where records are held by third parties or in other jurisdictions, in which case the access rights

described in Part C must be secured. Digital asset registrants must additionally maintain the tamper-evident monitoring records described in Part G.

36. Education and Training

- 116.** All employees must receive AML/CFT/CPF training on induction and on an ongoing basis, covering: the policies and procedures for the identification, record-keeping, detection and internal reporting of unusual and suspicious activity; and the legislative framework relating to identified risks, including ML, TF and PF. Training must be role-specific (onboarding and client-facing staff, operations and settlements, traders, registrar and transfer-agency staff, technology staff operating monitoring systems, senior management and the board each require tailored content) and must be refreshed at least annually, with completion tracked and tested. Training should incorporate the typologies and indicators in this Guidance, Bahamian case examples where available, and, for digital asset registrants, on-chain typologies. The CO and MLRO require deeper, continuing professional development commensurate with their responsibilities.

PART I: SUPERVISION, EFFECTIVENESS AND ENFORCEMENT

37. The Commission's Supervisory Approach

- 117.** The Commission supervises AML/CFT/CPF compliance on a risk-based cycle under a two-stream examination model, as described in the Commission's published statement, *Our Approach to Examinations*: focused AML/CFT/CPF examinations, scheduled on their own cycle keyed to the regulated person's ML/TF/PF risk rating; and full-scope examinations covering all other supervisory areas, keyed to the Commission's prioritisation framework. The two streams carry separate cycles and do not reset one another. The Commission additionally conducts for-cause examinations (with reason, outside the normal cycle, including on credible information of improper conduct) and thematic examinations (assessing compliance and best practice in a particular area across a population of firms). Examination testing routinely includes: the risk management framework and the Self-Risk Assessment; AML/CFT/CPF policies and procedures; CO and MLRO registration, seniority and independence; onboarding, CDD sampling and customer risk-rating reperformance; PEP policies, registers and files; sanctions screening and declaration compliance; transaction sampling and monitoring calibration; STR policies and records; training; record-keeping (including closed files); and complaints handling.
- 118.** Regulated persons should treat examination preparedness as a by-product of effective operation, not a separate exercise: if the evidence described in the "Commission's Expectations" boxes throughout this Guidance exists as a matter of course, examinations will find it. The Commission will share thematic observations with industry so that lessons from examinations raise standards across each sector.

38. Enforcement

- 119.** Failure to comply with the FTRA, the POCA, the ATA or the applicable sector Rules exposes a regulated person and its officers to criminal penalties and to administrative sanctions, including monetary penalties (up to the amounts prescribed for entities and individuals under the applicable framework), directions, restrictions, suspension or revocation of licences and registrations, and other remediation the Commission considers warranted. The published schedule of administrative penalties is available on the Commission's website. In determining its response, the Commission has regard to the nature, seriousness and duration of the breach; whether it was self-identified and self-reported; the quality of cooperation and remediation; and the regulated person's history. Prompt, candid self-reporting with credible remediation is consistently treated as a significant mitigating factor.

39. Interpretation and Review of this Guidance

- 120.** The Commission keeps this Guidance under review and will amend it to reflect legislative change, evolving FATF standards and typologies, examination findings, and industry feedback received through the Commission's ordinary engagement channels. Questions of interpretation, and suggestions for improvement, should be directed to the Commission through its published

contact channels. Regulated persons should ensure their policies are mapped to this Guidance and updated within a reasonable period (ordinarily not exceeding six months) following any material revision.

APPENDIX A: APPLICABILITY MATRIX

The table below maps each category of regulated person to its governing Act and its sector AML/CFT/CPF Rules. All regulated persons are additionally subject to the FTRA, the Financial Transactions Reporting Regulations, the Financial Transactions Reporting (Wire Transfers) Regulations, the POCA, the ATA and the International Obligations (Economic and Ancillary Measures) Act. Each set of 2026 Rules was gazetted on 27 October 2026.

Category of Regulated Person	Governing Act	Sector AML/CFT/CPF Rules
Registered firms and persons conducting registrable securities business	Securities Industry Act, 2024	Securities Industry (AML/CFT/CPF) Rules, 2026 (revoking and replacing the 2015 Rules)
Licensed investment funds and investment fund administrators	Investment Funds Act, 2019	Investment Funds (AML/CFT/CPF) Rules, 2026
Financial and corporate service providers (including TCSP activity)	Financial and Corporate Service Providers Act, 2020	Financial and Corporate Service Providers (AML/CFT/CPF) Rules, 2026 (revoking and replacing the 2019 Rules)
Digital asset businesses and registered exchanges	Digital Assets and Registered Exchanges Act, 2024	Digital Assets and Registered Exchanges (AML/CFT/CPF) Rules, 2026 (revoking and replacing the 2022 Rules)

Where a person holds multiple licences or registrations, each set of Rules applicable to the activities conducted under the relevant licence or registration applies, and the applicable requirements apply cumulatively.

APPENDIX B: ILLUSTRATIVE LIST OF BAHAMIAN DOMESTIC PEPs

Consistent with the FTRA, the FATF Recommendations and the Wolfsberg Group guidance, the classification of domestic PEPs should include, but is not limited to, individuals entrusted with the following prominent public functions:

- Head of State or Head of Government;
- Cabinet Ministers and Ministers of State;
- Members of Parliament and Members of the Senate;
- senior government officials, including Permanent Secretaries and heads of government departments and agencies;
- senior judicial officials, including Justices of the superior courts;
- senior military and police officials of flag, general or commissioner rank and their immediate deputies;
- Ambassadors, High Commissioners and other heads of diplomatic missions;
- senior executives of state-owned corporations and enterprises;
- senior officials of major political parties; and
- all individuals required by law to file financial disclosures with the Public Disclosure Commission under the Public Disclosure Act, 1976 and the Public Disclosure Act (Application to Public Appointees and Public Officers) Notice, 1980, including public officers listed in the Schedule to the Notice, and public appointees (Cabinet-approved appointments to public boards and committees, and appointments under statutory or other powers to positions of public influence or authority).

Where a role or relationship is not identified on this list, the regulated person is expected to apply a principles-based assessment and due diligence to classify the customer appropriately and assign a risk rating commensurate with the risk posed.

APPENDIX C: PEP DECLASSIFICATION CHECKLIST

Before declassifying any PEP, family member or close associate, the file should evidence each of the following:

- confirmation, from reliable sources, that the individual no longer holds the prominent public function, with the cessation date recorded;
- for domestic PEPs, that no less than twenty-four months have elapsed since cessation of the function;
- assessment of linkage to high-risk industries (financial and quasi-financial services; VASPs; casinos, gambling and gaming; real estate and property development; DNFBPs; precious metals, gems and high-value goods; arms, dual-use goods and high-risk trade; cash-intensive businesses; cross-border trade and shipping);
- assessment of position-specific risks, including the sphere of influence and function of the position previously held;
- assessment of tenure in office and of the likelihood of re-entry into public life (public activity, financial capacity, continuing political connections);
- assessment of source of wealth, particularly wealth acquired while in office, and of the plausibility of the risk profile and declared net worth;
- adverse media review, with any findings investigated and resolved;
- for former foreign PEPs, evaluation of corruption risk in the country concerned;
- senior management review and approval, documented and retained; and
- retention of prior PEP status on the customer record for investigative purposes, and an entry in the declassification log.

APPENDIX D: CONSOLIDATED PF RED-FLAG INDICATORS

The indicators below consolidate those in Part F for use in monitoring design and training. A single indicator warrants further monitoring; multiple indicators warrant thorough examination and consideration of reporting.

Customer profile

- vague or incomplete information about proposed trading activities; reluctance to elaborate when queried;
- customer, owners or senior managers appear in sanctions lists, negative news, or investigations or convictions;
- connections to a country of proliferation or diversion concern;
- dealing in dual-use goods, export-controlled goods, or complex equipment without technical background, or incongruent with stated activity;
- previous violations of dual-use or export control regimes;
- complex trade deals involving numerous third-party intermediaries in unrelated lines of business;
- commercial business behaving as a money-remittance or pay-through operation without clear rationale;
- affiliation with a university or research institution combined with dual-use goods trading;
- desire to use cash for industrial items or trade transactions.

Account and transaction activity

- transactions by or to persons ordinarily resident or domiciled in a country of proliferation or diversion concern;
- transactions involving items controlled under dual-use or export control regimes;
- involvement of companies with non-transparent ownership, front companies or shell companies;
- long account dormancy followed by a surge of activity;
- counterparties sharing owners, management, physical address, IP address or telephone number, or coordinating activity;
- circuitous transaction routing;
- involvement of financial institutions in countries with weak UNSCR implementation, FATF standards or export controls;
- sudden influxes of cash deposits followed by cash withdrawals;
- ledger arrangements structured to avoid frequent international financial transactions;
- personal accounts used to purchase industrial or export-controlled items.

Trade finance

- letters of credit requested for dual-use or export-controlled shipments before account approval;
- inconsistencies between trade documents and financial flows (names, addresses, final destination);
- freight forwarder listed as the product's final destination;
- wire instructions or payments from or to entities not identified on the original letter of credit or documentation.

Maritime, shipping and intermediaries

- deceptive shipping practices, including manipulation or disabling of vessel tracking systems, ship-to-ship transfers, flag hopping and vessel identity or document fraud;
- trade or payments involving vessels, shipping companies or ship managers with opaque ownership or links to sanctioned trade;
- intermediaries, brokers or front companies in third countries interposed without commercial rationale, or beneficial ownership that cannot be established;
- IP addresses or connection data inconsistent with the customer's stated location or profile;
- payment flows consistent with the earnings of undisclosed overseas information technology workers.

Digital assets

- direct or indirect exposure, within a risk-appropriate hop limit, to designated persons, ransomware actors, darknet markets or illicit protocols;
- use of mixers, privacy pools, coinjoin software or chain-hopping consistent with sanctions evasion;
- Travel Rule information conflicting with verified on-chain attribution, or missing, incomplete or altered metadata;
- exposure to wallet clusters attributed to thefts or hacks of virtual asset businesses by state-sponsored actors;
- structuring of transfers immediately below reporting or Travel Rule thresholds;
- rapid sequential cross-asset or cross-chain movement without economic rationale.

APPENDIX E: REFERENCE MATERIALS

In preparing this Guidance the Commission had regard to, and regulated persons may usefully consult, the following standards and publications (each as amended or updated from time to time):

- FATF: International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation (the FATF Recommendations and Methodology); Guidance on Politically Exposed Persons (Recommendations 12 and 22) (2013); Guidance on Proliferation Financing Risk Assessment and Mitigation; Comprehensive Update on Terrorist Financing Risks (2025); Complex Proliferation Financing and Sanctions Evasion Schemes (2025); Risk-Based Approach Guidance for the Securities Sector; Updated Guidance for a Risk-Based Approach to Virtual Assets and VASPs; and reports on ML/TF in the securities sector
- CFATF: mutual evaluation reports, typologies and guidance concerning The Bahamas and the region
- IOSCO: Objectives and Principles of Securities Regulation, and related AML/CFT reports and guidance for securities regulators
- Group of Financial Services Regulators (The Bahamas): Guidelines on Countering Proliferation Financing (2025)
- Wolfsberg Group: Guidance on Politically Exposed Persons
- Transparency International: Corruption Perceptions Index.

APPENDIX F: GLOSSARY OF ABBREVIATIONS

Abbreviation	Meaning
AML/CFT/CPF	Anti-money laundering, countering the financing of terrorism and countering proliferation financing
ATA	Anti-Terrorism Act, 2018
CDD / EDD / SDD	Customer due diligence / enhanced due diligence / simplified due diligence
CFATF	Caribbean Financial Action Task Force
CO / MLRO	Compliance Officer / Money Laundering Reporting Officer
DARE	Digital Assets and Registered Exchanges Act, 2024
DNFBP / TCSP	Designated non-financial business and profession / trust and company service provider
FATF	Financial Action Task Force
FCSPA	Financial and Corporate Service Providers Act, 2020
FIU	Financial Intelligence Unit
FTRA	Financial Transactions Reporting Act, 2018
GFSR	Group of Financial Services Regulators
IFA	Investment Funds Act, 2019
IO	FATF Immediate Outcome
IOEAMA	International Obligations (Economic and Ancillary Measures) Act
IRF	Identified Risk Framework
ML / TF / PF	Money laundering / terrorist financing / proliferation financing
NRA	National Risk Assessment
PEP	Politically exposed person
POCA	Proceeds of Crime Act, 2018
SIA	Securities Industry Act, 2024
SRA	Self-Risk Assessment (the business-wide ML/TF/PF risk assessment required under the FTRA)
STR	Suspicious transaction report
TFS	Targeted financial sanctions
UNSCR	United Nations Security Council Resolution
VASP	Virtual asset service provider