SECURITIES COMMISSION OF THE BAHAMAS

GUIDANCE NOTE

SELF-RISK ASSESSMENTS

Money Laundering, Terrorist Financing and Proliferation Financing

PUBLISHED DATE: 12 AUGUST 2026

GUIDANCE NOTE ON SELF-RISK ASSESSMENTS

Money Laundering, Terrorist Financing and Proliferation Financing

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

TABLE OF CONTENTS

PART A — INTRODUCTION AND FRAMEWORK

1. Introduction

1. This Guidance Note sets out the expectations of the Securities Commission of The Bahamas (the "Commission") regarding the conduct, documentation, approval, maintenance and use of self-risk assessments by its registrants and licensees. A self-risk assessment (an "SRA") is the assessment that each registrant is required to conduct of its own exposure to money laundering ("ML"), terrorist financing ("TF") and proliferation financing ("PF") risks, having regard to the nature, scale and complexity of its business. The SRA is the assessment referred to in the FATF Recommendations, and in a number of other jurisdictions, as the business risk assessment or business-wide risk assessment.

2. The SRA is the foundation of the risk-based approach. It is the instrument by which a registrant identifies where its ML/TF/PF risks concentrate and, in consequence, where its preventive measures — customer due diligence, enhanced due diligence, monitoring, screening, training and resourcing — must be calibrated. A registrant that has not properly understood its own risks cannot properly mitigate them, and the adequacy of every downstream control is judged by reference to the risk analysis that ought to underpin it.

3. This Guidance Note is issued to promote a consistent and adequate standard of self-risk assessment across the Commission's regulated population, to inform registrants of the criteria against which their SRAs will be assessed during examinations and supervisory reviews, and to assist registrants — in particular smaller registrants — in producing SRAs that are proportionate, meaningful and genuinely their own.

2. Purpose and Status of this Guidance

4. The Commission will have regard to this Guidance Note when assessing the adequacy of a registrant's SRA during examinations conducted by the Examinations Department, during supervisory reviews conducted by the Supervision Department, and upon any request by the Commission for production of the SRA. A registrant's SRA is reviewable **at examination and on request** (FTRA, section 5(1)(e)); there is no standing requirement to file the SRA with the Commission, but registrants must be able to produce the current, approved version promptly when required.

5. The Commission has issued companion documents alongside this Guidance Note: an **SRA Template and Illustrative Structure** and an **SRA Risk Assessment Matrix** workbook. These are illustrative aids, not mandatory forms. **Use of the template or the matrix does not of itself constitute compliance.** The Commission assesses the adequacy of an SRA against the registrant's actual risk profile, and a templated document that has not been genuinely adapted to the registrant's own business will not satisfy the obligation. Conversely, a registrant may prepare and produce its SRA in any format — its own design, a group format,

or one prepared by or with an external consultant — and will not be criticised for that choice, provided the assessment covers, at a minimum, the areas required by this Guidance Note.

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

3. Applicability

7. This Guidance Note applies to all registrants and licensees of the Commission that are subject to AML/CFT/CPF obligations, including persons registered or licensed under the Securities Industry Act, 2024, the Financial and Corporate Service Providers Act, 2020, and the Digital Assets and Registered Exchanges Act, 2024, and investment fund administrators and other service providers licensed under the Investment Funds Act, 2019, other than registered investment fund managers in that capacity (together, "registrants"). **Investment funds and registered investment fund managers are not within the scope of this Guidance Note in their capacity under the Investment Funds Act, 2019**: the ML/TF/PF risks associated with a fund are assessed within the SRA of its administrator and of any other registrant providing services to the fund. This carve-out is not an exemption from AML/CFT/CPF obligations: a fund manager or other person registered under the Securities Industry Act, 2024 remains fully within the scope of this Guidance Note as an SIA registrant in respect of its business. Registrants conducting virtual asset activities should note that FATF Recommendation 15 and its Interpretive Note apply Recommendation 1 to virtual asset service providers in full, and that the risk factors relevant to digital asset business are addressed further in this Guidance Note and its companion documents.

8. This Guidance Note does not create new legal obligations. It explains how the Commission interprets and will supervise existing obligations. In the event of any inconsistency between this Guidance Note and the governing legislation, the legislation prevails.

4. Legislative and Regulatory Basis

9. The obligation to conduct a self-risk assessment arises under Part II, section 5 of the **Financial Transactions Reporting Act, 2018** ("FTRA"), which requires every financial institution to take appropriate measures to identify, assess and understand its ML, TF and PF risks in relation to (i) its facility holders and the countries or jurisdictions of their origin, (ii) the countries or jurisdictions of its operations, and (iii) its products, services, transactions and delivery channels; to develop and implement a comprehensive risk management system approved by senior management; to take account of any risk assessment carried out at a national level and any regulatory guidance issued; to document the outcome of its risk assessments in writing and keep them up to date; and, upon request, to provide the Commission with a copy of its risk assessment. These obligations operate alongside the

Financial Transactions Reporting Regulations, 2018, the Proceeds of Crime Act, 2018 and the Anti-Terrorism Act, 2018, and, in respect of proliferation financing, the framework governing targeted financial sanctions.

10. The obligation reflects **Recommendation 1** of the Financial Action Task Force ("FATF") and its Interpretive Note, which require financial institutions and designated non-financial businesses and professions to take appropriate steps to identify and assess their ML/TF risks, and — following the 2020 amendments to Recommendation 1 — to identify and assess the risk of potential breach, non-implementation or evasion of the targeted financial sanctions obligations relating to proliferation financing.

PART B — CORE EXPECTATIONS

11. The expectations in this Part apply to **every registrant, regardless of size**. No registrant is exempt from any element. Part C explains how the depth of analysis required under each element scales with the nature, scale and complexity of the registrant's business.

5. Governance and Ownership

12. The SRA must be owned by the registrant. Responsibility for the SRA rests with the registrant's board of directors or equivalent senior governing body, which must approve the SRA and each material revision of it. The compliance officer or money laundering reporting officer will ordinarily lead its preparation, and a registrant may engage an external consultant to conduct or assist with the SRA. In every case the registrant remains fully responsible for the content and conclusions: the assessment must be informed by the registrant's own knowledge and data, and the governing body must be able to demonstrate that it understands and has challenged the assessment it has approved.

6. Methodology

13. The SRA must record the methodology by which it was produced: the risk factor categories considered, the sources of information relied upon, the scales used to rate risk, the manner in which the effectiveness of controls was assessed, and the basis on which residual risk conclusions were reached. The methodology need not be elaborate, but it must be stated, so that a reviewer can understand how the registrant moved from information to conclusion.

14. Relevant sources of information include, at minimum: the registrant's own client, product and transaction data; the most recent National Risk Assessment of The Bahamas and any sectoral risk assessments issued by Bahamian authorities; typologies and guidance published by the FATF, the Caribbean Financial Action Task Force and the Financial Intelligence Unit; and the registrant's own experience, including internal suspicious activity escalations and the outcomes of prior examinations or audits.

7. Risk Factor Categories

15. The SRA must assess, at minimum, each of the following categories of risk factor as they apply to the registrant's business:

- **Customer risk** — the nature of the client base, including client types (natural persons, corporate vehicles, trusts and other legal arrangements, nominee relationships), the presence of politically exposed persons, non-resident clients, clients with complex or opaque ownership structures, and clients in higher-risk occupations or industries;
- **Product, service and transaction risk** — the inherent vulnerability of the products and services offered, including features such as anonymity or pseudonymity, cross-border reach, rapid movement of value, third-party funding, leverage, and (for digital asset business) exposure to unhosted wallets, mixing or anonymity-enhancing technologies;

- **Delivery channel risk** — the manner in which clients are onboarded and served, including non-face-to-face onboarding, reliance on intermediaries, introducers or agents, and reliance on third parties for elements of customer due diligence;
- **Geographic risk** — assessed in the two dimensions required by section 5(1)(a) of the FTRA: the countries or jurisdictions of origin of the registrant's facility holders and their beneficial owners, and the countries or jurisdictions of the registrant's own operations — together with the jurisdictions connected through counterparties, transaction flows and service providers, having regard to jurisdictions identified by the FATF as subject to a call for action or increased monitoring, jurisdictions subject to sanctions, and jurisdictions otherwise assessed as presenting higher ML/TF/PF risk.

16. The customer risk assessment must additionally address the registrant's obligations under section 14 of the FTRA in respect of politically exposed persons: the risk-management systems for identifying politically exposed facility holders and beneficial owners prior to establishing or continuing the relationship, the measures for establishing source of wealth and source of funds, and enhanced ongoing monitoring of such relationships.

17. Registrants should also consider any other factor material to their particular business, such as the pace of business growth or change, reliance on outsourcing and third-party service providers, the adoption of new or developing technologies, significant events or developments in the management and operations of the registrant or its group, and staffing or capacity constraints in the compliance function. The Commission does not require these operational matters to be assessed as a separate standing risk category: they are considered within the categories above and under the review triggers in section 11.

8. Proliferation Financing

18. The SRA must include an assessment of proliferation financing risk. At minimum, this comprises an assessment of the risk that the registrant's products, services, clients or geographic exposures could be used to breach, evade or fail to implement targeted financial sanctions relating to proliferation financing. The PF assessment may be integrated within the same document as the ML/TF assessment, but its conclusions must be separately identifiable; an SRA that is silent on PF is incomplete.

9. Inherent Risk, Controls and Residual Risk

19. The SRA must distinguish between **inherent risk** (the risk present in the business before controls are applied), the **mitigating controls** in place, and **residual risk** (the risk remaining after the effect of those controls is taken into account). The assessment of controls must be honest: a control that exists on paper but is known to operate weakly — for example, a screening system generating unmanageable alert backlogs, or monitoring rules never tuned to the business — must be weighted accordingly. An SRA in which every control is rated fully effective and every residual risk is rated low will attract supervisory scepticism.

10. Documentation

20. The SRA must be documented in writing, dated, version-controlled, and retained together with the material information relied upon. The document must state its conclusions clearly: which areas of the business carry the highest residual ML/TF/PF risk, and what the registrant intends to do about them. A collection of scoring tables without narrative analysis and conclusions does not constitute an adequate SRA.

11. Review, Currency and Trigger Events

21. 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 registrant's own compliance function; publication of a new or revised National Risk Assessment or relevant sectoral assessment; and any significant ML/TF/PF event affecting the registrant. 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.

12. Use of the Assessment

22. The SRA must demonstrably drive the registrant's AML/CFT/CPF programme. The registrant's policies and procedures, its client risk-rating model, the calibration of enhanced due diligence and ongoing monitoring, its training programme and its compliance resourcing should each be traceable to the conclusions of the SRA. During examinations, the Commission will test this linkage; a well-drafted SRA that bears no visible relationship to the registrant's actual controls will be treated as a deficiency in both.

Commission's Expectations — Evidencing the SRA in Practice

- The governing body has approved the SRA and each material revision, with evidence of review and challenge, and can explain its conclusions.
- The methodology is stated, so that a reviewer can retrace the route from the registrant's own information to its conclusions.
- The control assessment is honest: known weaknesses are weighted, and uniformly favourable ratings are supported by evidence.
- The document is dated and version-controlled, with annual reviews and section 5(2) pre-launch assessments evidenced in writing.
- Policies, the client risk-rating model, monitoring calibration, training and resourcing are each traceable to the SRA's conclusions.

PART C — PROPORTIONALITY

13. The Single Standard, Applied Proportionately

23. The Commission applies a **single standard, proportionately**. It does not operate tiered or simplified SRA regimes, and registrants are not required — and not able — to elect into a reduced standard by reference to their size. The depth, sophistication and length of the analysis expected under each element of Part B scales with the **nature, scale and complexity of the registrant's business and the risks to which it is exposed** — not with headcount or revenue alone.

24. In practice, a registrant with a simple, domestic, low-risk business model may satisfy these expectations in a concise document, and the illustrative structure at Appendix A and in the companion SRA Template shows what an adequate concise SRA can look like. Conversely, a small registrant with a high-risk profile — for example, a firm serving non-resident clients through complex structures, or conducting digital asset business with cross-border exposure — must produce an assessment whose depth matches those risks, however small the firm. **Size is not a proxy for risk**, and the test the Commission applies is in every case the same: is this SRA adequate for this registrant's actual risk profile?

Commission's Expectations — Proportionality

- The same elements apply to every registrant; proportionality changes the depth required, never the coverage.
- A concise SRA that is genuinely the registrant's own — its own data, an honest control view, a real conclusion — can satisfy the standard.
- Length and production values earn no credit: a substantial document that is generic or unconnected to the firm's data does not.
- The constant test: is this SRA adequate for this registrant's actual risk profile?

PART D — GROUPS, THIRD PARTIES AND COMMON DEFICIENCIES

14. Group Structures and Use of Third Parties

25. A registrant that is part of a group may draw upon a group-level risk assessment, but may not simply adopt it. The registrant must ensure that its SRA specifically assesses the risks of its Bahamian business and operations, reflects Bahamian legal obligations and the Bahamian National Risk Assessment, and reaches conclusions at the level of the regulated entity. A group document that does not descend to the level of the Bahamian registrant will not satisfy the obligation.

26. Where consultants or other third parties conduct or assist in preparing the SRA, the analysis must reflect the registrant's actual business rather than generic sector content. The Commission is familiar with commercially available SRA products and will look behind the format to the substance. Indicators that an assessment is not genuinely the registrant's own — sector boilerplate untouched by the firm's data, risk ratings unconnected to the client book, conclusions that could describe any firm — will be treated as evidence of inadequacy.

15. Common Deficiencies

27. Registrants' attention is drawn to deficiencies commonly identified by supervisors and assessment bodies internationally, each of which the Commission will regard as indicative of an inadequate SRA:

- absence of any documented SRA, or an SRA so out of date that it no longer describes the business;
- omission of one or more required risk factor categories, most frequently geographic risk or proliferation financing;
- failure to distinguish inherent from residual risk, or uniform ratings applied without analysis;
- controls assessed as effective without any evidence of testing or regard to known weaknesses;
- generic or templated content not adapted to the registrant's actual clients, products and data;
- no governing-body approval, or approval unaccompanied by any evidence of review or challenge;
- no linkage between the SRA's conclusions and the registrant's policies, client risk model, monitoring or resourcing;
- no review following material business change, such as the launch of a new product or entry into digital asset activity.

PART E — SUPERVISION AND COMPANION INSTRUMENTS

16. Supervisory Approach and Consequences

28. The adequacy of the SRA is assessed within AML/CFT/CPF examinations and may also be assessed by the Supervision Department outside the examination cycle, including by requiring production of the SRA on request. The Commission's assessment considers both the **quality of the document** — coverage, methodology, honesty of the control assessment, clarity of conclusions — and the **quality of its use** — whether the registrant's programme in fact reflects it.

29. The outcome of the Commission's assessment of a registrant's SRA informs the registrant's risk profile within the Commission's risk-based supervisory framework and may accordingly affect the intensity and frequency of future supervisory attention. Material inadequacy in an SRA constitutes a breach of the registrant's obligations and may result in remedial directions, follow-up examination or enforcement action, according to the seriousness of the deficiency.

17. Companion Instruments and Assistance

30. The following companion documents are issued or maintained in connection with this Guidance Note: the **SRA Template and Illustrative Structure**, which guides registrants step by step through producing the written assessment and illustrates what an adequate concise SRA can look like for a simple, lower-risk business; and the **SRA Risk Assessment Matrix**, an Excel workbook providing sector-specific risk sheets — with each risk factor explained in plain language for the relevant licence type — and a step-by-step path from scoring inherent risk, control effectiveness and residual risk to the written conclusions of the SRA. Both are voluntary aids and are subject to the caution in paragraph 5 of this Guidance Note.

31. **Appendices B to D** set out sector-specific risk factors that registrants in the relevant sectors must consider in their SRAs, supplementing (not replacing) the risk factor categories in Part B. Where a registrant conducts business in more than one sector, each applicable appendix applies. The appendices will be revised as typologies and the national and sectoral risk assessments of The Bahamas evolve.

32. Enquiries concerning this Guidance Note may be directed to the Supervision Department of the Commission.

APPENDIX A — ILLUSTRATIVE STRUCTURE OF A SELF-RISK ASSESSMENT

The following outline illustrates one acceptable structure for an SRA. It is indicative only; registrants may adopt any structure that meets the expectations of this Guidance Note. Section references are to this Guidance Note.

1. Executive summary and conclusions — the registrant's overall residual ML/TF/PF risk conclusions and the highest-risk areas identified, stated plainly.

2. Business overview — the registrant's licences and registrations, products and services, client base, delivery channels, geographic footprint, and any material recent or planned changes.

3. Methodology and information sources — scales used, how control effectiveness was judged, and the internal and external sources relied upon (section 6).

4. Risk assessment by category — for each of customer, product/service/transaction, delivery channel and geographic risk: inherent risk analysis grounded in the registrant's own data; the relevant controls and an honest assessment of their effectiveness; and the residual risk conclusion (sections 7 and 9).

5. Proliferation financing assessment — the assessment required by section 8, with separately identifiable conclusions.

6. Other material factors — outsourcing, new technology, growth or capacity considerations, where relevant.

7. Action plan — remediation or enhancement actions arising from the assessment, with owners and target dates.

8. Governance record — preparation and review history, and the record of governing-body challenge and approval, dated and versioned (sections 5, 10 and 11).

APPENDIX B — SECTOR RISK FACTORS: DIGITAL ASSET BUSINESSES

This Appendix applies to persons registered under the Digital Assets and Registered Exchanges Act, 2024 and to any other registrant whose business involves digital asset activities. It supplements Part B of this Guidance Note and should be read with FATF Recommendation 15 and its Interpretive Note, the FATF guidance on virtual assets and virtual asset service providers, the FATF report on red flag indicators of money laundering and terrorist financing involving virtual assets, and any guidance issued by the Commission concerning the travel rule.

Inherent profile. Digital asset business combines near-instant cross-border transferability, pseudonymity, global reach without physical presence, transaction irreversibility and rapid product evolution. These features elevate inherent ML/TF/PF exposure relative to traditional securities business, and a digital asset registrant's SRA is expected to reflect that starting point. In particular, the exploitation of virtual assets by sanctioned state actors — including through cyber-theft and the laundering of stolen assets — is an established typology, and a digital asset SRA that rates PF risk as negligible without analysis will not be accepted as adequate.

Risk factors to be considered include, at minimum:

- **Products, services and transactions** — the custody model (custodial or non-custodial); exchange between digital assets and fiat and between digital assets; transfer services; token issuance or participation in issuances; staking, lending and yield products; stablecoin exposure; exposure to anonymity-enhanced assets, privacy wallets, mixers and tumblers; interaction with DeFi protocols and cross-chain bridges; and the process for onboarding new tokens or assets;
- **Customers** — expected use of unhosted wallets; clients transacting with high-risk counterparties identified through analytics; nested services, OTC desks and brokers as clients; and clients whose asset provenance (for example early acquisition or mining) is difficult to evidence;
- **Delivery channels** — wholly non-face-to-face onboarding; reliance on digital identity solutions; programmatic or API access; and agents and introducers;
- **Geography and counterparties** — exposure to counterparty service providers in jurisdictions with weak or absent virtual asset regulation, including jurisdictions where travel rule obligations are not yet implemented; FATF-listed jurisdictions; and sanctioned jurisdictions;
- **On-chain exposure** — exposure to the proceeds of ransomware, darknet markets, frauds and thefts through incoming flows; and rapid layering through multiple wallets or chains;
- **Proliferation financing** — exposure to sanctioned actors' documented use of virtual assets, and the adequacy of wallet and counterparty screening against that exposure.

The Commission expects a digital asset registrant's SRA to address how on-chain exposure is identified and measured, including through blockchain analytics capability proportionate to the business model, and to treat travel rule compliance risk as a distinct counterparty and delivery-channel factor.

APPENDIX C — SECTOR RISK FACTORS: FINANCIAL AND CORPORATE SERVICE PROVIDERS

This Appendix applies to persons licensed under the Financial and Corporate Service Providers Act, 2020. The sector spans two limbs — the provision of financial services, and the provision of corporate and legal-arrangement services — and the risk profiles of the two differ materially. A licensee conducting both must assess each limb distinctly; the FATF's risk-based approach guidance for trust and company service providers is directly relevant to the second limb.

Risk factors to be considered include, at minimum:

- **Corporate and legal-arrangement services** — formation of companies, including for non-resident clients; provision of registered office, registered agent or business address; provision of nominee shareholders or directors; acting as, or arranging, trustees or protectors; establishment of multi-jurisdictional structures with layered ownership; supply of ready-made or aged entities; and services marketed on speed or discretion of formation;
- **Customers** — non-resident clients acquiring Bahamian vehicles; wealth structuring connected to politically exposed persons; clients introduced by foreign professional intermediaries with limited or no direct contact; and beneficial owners located in higher-risk jurisdictions;
- **Structure purpose** — structures whose principal apparent function is to obscure ownership or control, including chains of legal persons across jurisdictions, extensive powers of attorney, and arrangements separating legal and beneficial ownership without commercial rationale;
- **Delivery channels** — chains of introducers; reliance on third parties, particularly foreign professionals, for customer due diligence; and non-face-to-face onboarding;
- **Financial services limb** — cash intensity, third-party payments and receipts, and lending or broking activity conducted for clients whose source of funds is difficult to establish;
- **Proliferation financing** — the use of legal persons and arrangements to obscure sanctioned beneficial ownership, and the formation of front companies capable of supporting procurement activity.

The size of an FCSP is a poor proxy for its risk. A small licensee administering complex cross-border structures for non-resident beneficial owners carries a substantial inherent profile, and its SRA must be correspondingly substantial (section 13 of this Guidance Note).

APPENDIX D — SECTOR RISK FACTORS: SECURITIES BUSINESS AND INVESTMENT FUND SERVICES

This Appendix applies to persons registered under the Securities Industry Act, 2024 and to investment fund administrators and other service providers licensed under the Investment Funds Act, 2019 (other than registered investment fund managers in that capacity). Investment funds and registered investment fund managers (in their IFA capacity) are outside the scope of this Guidance Note; a fund manager registered under the Securities Industry Act, 2024 applies this Appendix as an SIA registrant. The fund-related factors below are assessed from the perspective of the administrator or service provider whose SRA is being prepared.

Risk factors to be considered include, at minimum:

- **Products and transactions** — layering of value through the purchase and sale of securities; low-liquidity or low-priced securities capable of transferring value or supporting manipulation-based laundering; wash trades and matched orders; transfers of securities between apparently unrelated accounts; journal transfers between accounts; free-credit and margin balances used as a store of value; and any residual physical securities exposure;
- **Investment funds** — funds with concentrated non-resident investor bases; subscriptions or redemptions involving third-party payers or payees; subscriptions in kind; tolerance of early redemption at cost to the investor; and fund vehicles used for private wealth structuring with nominee or opaque features;
- **Customers** — intermediated and omnibus account structures that obscure underlying clients; institutional clients from jurisdictions with weak regulation; and corporate vehicles or legal arrangements as accountholders;
- **Delivery channels** — reliance on administrators, sub-distributors, introducing brokers or other intermediaries for elements of customer due diligence, and the risk inherent in that reliance itself;
- **Geography** — the jurisdictions of the investor base, of intermediaries relied upon, and of subscription and redemption flows;
- **Proliferation financing** — securities or custody accounts used to hold or move value for sanctioned persons, including through intermediated structures that impede the identification of underlying parties.

Where reliance is placed on an administrator or other intermediary for customer due diligence, the SRA must assess the reliance risk explicitly: the quality of the intermediary's framework, the jurisdiction of its supervision, and the registrant's ability to obtain underlying information without