FINANCIAL SERVICES AUTHORITY

SAINT VINCENT & THE GRENADINES

**GUIDELINES:**

# ONGOING MONITORING GUIDELINES

**Issued: September 2025**

## TABLE OF ACRONYMS

| | |
|---|---|
| AML | Anti- Money Laundering |
| BO | Beneficial Owner |
| CDD | Customer Due Diligence |
| CFATF | Caribbean Financial Action Task Force |
| CFT | Counter-Financing of Terrorism |
| DNFBPs | Designated Non-Financial Business and Professions |
| EDD | Enhanced Due Diligence |
| FATF | Financial Action Task Force |
| FI | Financial Institution |
| FIU | Financial Intelligence Unit |
| FSA | Financial Services Authority |
| FSRB | FATF Styled Regional Body |
| ML | Money Laundering |
| MLRO | Money Laundering Reporting Officer |
| PEP | Politically Exposed Person |
| PF | Proliferation Financing |
| RBA | Risk Based Assessment/ Approach |
| SARs | Suspicious Activity Reports |
| SDD | Simplified Due Diligence |
| SVG | St. Vincent and the Grenadines |
| TF | Terrorist Financing |

## INTRODUCTION

The non-banking financial sector in St. Vincent and the Grenadines is regulated and supervised by the FSA pursuant to the Financial Services Authority Act, No. 33 of 2011.

The following Guidelines are issued pursuant to section 10 of the Financial Services Authority Act. The guidance herein specifically addresses the ongoing monitoring approach to be applied by regulated entities in accordance with the AML/CFT legislation.

## OBJECTIVES

The objective of these guidelines is to:

- Provide comprehensive guidance to the non-bank and international financial services sector for the development and implementation of a risk-sensitive approach in determining the extent and nature of its ongoing monitoring of business relationships in accordance with the Anti-Money Laundering and Terrorist Financing Regulations of 2014 and its amendments ("the Regulations"), the Anti-Money Laundering and Terrorist Financing Code of 2017 ("the Code") and the Anti-Terrorism Act, 2023.

## SCOPE OF APPLICATION

These Guidelines apply to all service providers within the non-banking and international financial services sector in St. Vincent and the Grenadines, regulated by the Authority.

## PROVISO STATEMENT

The Ongoing Monitoring Guidelines are designed to guide service providers in applying the minimum standards for ongoing monitoring practices. It will form an integral part of the framework used by the FSA in assessing how licensees implement their AML/CFT policies.

The Guidelines provide general guidance in the application of the governing legislation and should not be misconstrued or referenced as the principal document for conducting effective ongoing monitoring. They should be read in conjunction with the Regulations, and the Code as well as any written directives, notices, circulars, and other guidelines issued by the FIU and or the FSA from time to time.

In formulating these Guidelines, the FSA did not consider the circumstances specific to any entity in isolation, as such, these Guidelines should be viewed as general information for the purpose of conducting ongoing monitoring. Each institution within the sector is required to review the guidance and tailor its policies, procedures, and processes accordingly.

## DEFINITIONS

***"Business Relationship"*** means a relationship established between a service provider and a client to conduct financial transactions or provide services relating to financial transactions.

***"Ongoing monitoring"***[1] means:

a. the scrutiny of transactions undertaken throughout the relationship, including, where necessary, the source of funds, ensuring that the transactions are consistent with the service provider's knowledge of the customer and the customer's business and risk profile, and

b. keeping the documents, data, or information obtained for the purposes of applying CDD measures up-to-date and relevant by undertaking systematic reviews of existing records, particularly for higher risk customers.

"***Enhanced ongoing monitoring****"* refers to ongoing monitoring measures that involve specific and appropriate action to compensate for the higher risk of ML or TF

***"Risk-based Approach to Monitoring"*** means the scope of monitoring would be linked to the risk profile of the customer.

"***High-risk jurisdiction"***[2] means a country with significant strategic deficiencies in its regimes to counter money laundering, terrorist financing, and proliferation financing and has been identified as having a higher risk by the FATF or another FSRB, or independent of such call by any of the foregoing.

## GOVERNING LEGISLATION

The responsibility of financial institutions to conduct ongoing monitoring is governed primarily by the Regulations. *Regulations 11 (5), 13 (1) (b), 14 (2), 20 (1), (a), 35E* and the Code *Paragraph 27 and its Guidance Note Page, 157 -160*.

### Conducting Ongoing Monitoring and Enhanced Ongoing Monitoring[3]

Service providers are required to conduct ongoing monitoring of their customers/business relationships.[4].

Service providers are also required to, on a risk-sensitive basis, undertake enhanced ongoing monitoring when certain factors exist.[5]

[1] Regulation 7,
[2] https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Call-for-action-february-2024.html
[3] Guidance Note – Enhance customer due diligence – introduction Page 108-112, AML/CFT Code, 2017
[4] Regulation 11(5).
[5] Regulation 14 (2) and (2a).

## ONGOING MONITORING

Ongoing monitoring is an essential part of the compliance process that supports effective AML/CFT systems, which must be developed and used to review information obtained about the customers of a service provider and transaction patterns in order to:

i. Detect changes in customer behaviour;

ii. Determine appropriate triggers for unusual or suspicious activities and the filing of suspicious activity reports with the FIU;

iii. Keep customer, beneficial ownership information, and the purpose and intended nature of the business relationship up to date

iv. Discern whether transactions or activities are consistent with the customer's risk assessment and risk profile; and

v. Guide the performance of subsequent reassessments of risk associated with the customer.

As such, service providers must establish appropriate ongoing monitoring policies and procedures to[6]:

- ✓ assess its customer's business and risk profile, and ensure that the authorization in place is appropriately designed and delegated;

- ✓ monitor all its customers' transactions/activity and behaviour, especially for customers categorized as high-risk[7]. The system implemented must effectively recognize and examine exceptional transactions/activity, trigger events, red flags.[8];

[6] Regulation 20 (b)

[7] Some examples of high-risk customers include, but are not limited to:

i. Politically Exposed Persons and their family members and associates.
ii. Non-face-to-face customers.
iii. Customers with complex ownership structures.
iv. Customers linked to high-risk countries.
v. Customers and activities identified based on the findings on the NRAs, sectoral risk assessments and institutional risk assessments.

[8] Trigger events/Red Flags are limits or indicators established as early warning signals that require mandatory review. These indicators should be informed by the ML/TF risk identified in the business risk assessment. Trigger events may include:

i. The identification or subsequent recognition of a politically exposed person ("PEP") in the business relationship.
ii. The identification of adverse information from sources such as media reports or other relevant sources.
iii. The customer requesting a new or higher risk product.
iv. Paying higher charges to keep their identity secret.
v. The customer appears to be acting on behalf of someone else and does not provide satisfactory information regarding whom they are acting for.
vi. The customer refuses to provide the Financial Institution ("FI") with relevant or accurate information about the nature and intended or ongoing purpose of the relationship.

It is beneficial for FI's to prepare a list of trigger events as a guide for staff. This must however be coupled with continuous training to aid staff in identifying new and emerging trigger events. Such a training programme promotes a risk-based approach and optimizes the effectiveness of transaction monitoring.

- ✓ recognize whether any business relationship or one-off transactions are directly or indirectly conducted with sanctioned persons, organisations or other parties and where necessary, collect appropriate additional information to determine whether the transaction or activity has an apparent economic or lawful purpose;

- ✓ examine and recognize transactions/activities with a person connected with higher-risk jurisdictions[9], review as far as possible their background and purpose of transactions/activity in the context of the business and risk profile, set forth its findings in writing and the mitigation strategies for the assessed risk;[10]

- ✓ undertake sanctions screening for all business relationships and one-off transactions. Screening should include the customer, the beneficial owner, and other associated parties. Screening should be carried out at the time of establishing the relationship, periodically, and when there is a trigger event;

- ✓ guide the frequency of reviews of accounts and internal controls to ensure that the AML policies remain robust. and

- ✓ ensure appropriate systems and controls are in place to comply with asset-freezing and reporting obligations "without delay" as issued by the FIU.

To demonstrate compliance with Regulations 11 (1) (b), and paragraph (xxxi) (c), the service providers must comply with page 106, paragraph (xxxii) (a-b) of the AML/CFT Code, 2017 which states:

a. review and update its customer due diligence information on at least and annual basis where it has assessed a customer relationship as presenting a high risk; and

b. review and update its customer due diligence information on a risk-sensitive basis, but not less than once in every three years, where it has assessed a customer relationship as presenting normal or low-risk,

## OVERSIGHT OF ON-GOING MONITORING

The financial institution or service provider is responsible for designating an appropriately qualified person who, among other things, will:

- ✓ assign responsible/personnel for ongoing monitoring activities

- ✓ investigate the background and purpose of all complex or unusually large transactions and unusual patterns of transactions that have no apparent economic or lawful purpose, and

[9] Countries that have significant strategic deficiencies in their counter ML/TF and PF
[10] Paragraph (xxvii), page 105, AML/CFT Code, 2017

- ✓ record the investigation findings and revise and update existing records as much as necessary, to adjust the customer business and risk profile and refine the monitoring parameters for the relevant customer.

- ✓ design reporting protocols for the ongoing monitoring programme for reporting to management/the Board of directors (board)

**Optimizing the Ongoing Monitoring Programme**

The method used for and appropriateness of ongoing monitoring systems depends on various factors including the:

i. nature of products and services offered;

ii. business practices including delivery channels;

iii. size and nature of the client base;

iv. risk level assigned to customers during the risk assessment process;

v. volume and value of transactions that occur within a specific period; and

vi. capacity of staff members involved in the processing and review of transactions/activities.

***Example: A client identified as posing a low risk may require less frequent monitoring, whereas those assessed as high risk will require more advanced ongoing monitoring.***

As such, a service provider must implement an ongoing monitoring mechanism, which:

- ✓ is commensurate with the size, nature and complexity of their business activities,

- ✓ is commensurate with the ML/TF/PF risks of the customer poses in accordance with page 106, paragraph (xxxii) (a-b) of the AML/CFT Code, 2017,

- ✓ enables timely and consistent analysis of customer transactions/activities,

- ✓ can systematically prioritize customer information reviews based on the customer's business risk and risk profile, and

- ✓ includes procedures for identifying trigger events/red flags and unusual patterns.

Transaction monitoring is important for detecting suspicious or unusual transaction patterns over time. This activity involves tracking transactions in real-time to detect unusual activities and analyzing transactions based on customer risk profiles, behaviour and trends.

A service provider may utilize manual transaction monitoring, automated transaction monitoring, or a blended approach for ongoing monitoring. Irrespective of the mode chosen, the service provider should establish procedures to regularly review its processes to ensure that its systems are operating appropriately and effectively and are sufficiently reliable to monitor and manage its MT/TF risk. Attention should be paid to instances of sudden large deposits, frequent small deposits (structuring), and any financial activity that is inconsistent with the customer's known behaviour.

**Specialized Software Tools[11]**

The use of specialised software to enhance monitoring activities is permissible and encouraged, particularly for entities that are considered systemic and engage in large-volume transactions. These tools can effectively automate and streamline the transaction monitoring process and integrate risk assessment and record-keeping processes more effectively and efficiently than a manual process. Software programmes should not be used to replace human resources but instead to complement same.

Where a service provider determines that a specialized software tool is more appropriate for its operations, the service provider should ensure compatibility with the inherent business risks, the institution's operating system, and how customer information, including transaction data, will be integrated into the tool. Further, service providers must ensure that the tool is adequately tailored to the risk and context of Saint Vincent and the Grenadines and that relevant staff are sufficiently trained to utilize the tool initially and on an ongoing basis.

**Manual monitoring**

Where a service provider determines that a manual approach is more appropriate for its operations, it must assess the capability of the manual controls to detect higher-risk activities. In this process, the service provider must ensure that it can retain all relevant records and audit evidence relating to the assessment of transactions undertaken by its customers. The manual approach also requires a certain level of competence from the regulated entity's staff members involved in the review of transactional activity. Focused training of staff will need to be undertaken at appropriate intervals.

**STRUCTURE OF ONGOING MONITORING ACTIVITIES:**

The ongoing monitoring processes of a service provider must be structured in such a way that staff is prompted when additional information is needed to confirm the identity or business purpose of the customer. The FIs should establish the types of additional information that can be requested for various scenarios.

A service provider should establish structured and definitive criteria to support its ongoing monitoring program. The programme should include but is not limited to:

[11] Note: the implementation of an automated transaction monitoring system does not eliminate the need for manual reviews. At a minimum, the entity's Money Laundering Reporting Officer ("MLRO") will be required to assess any potential suspicious activity and determine whether the matter should be escalated to the FIU. Further, the use of an automated system does not absolve a service provider of the need to ensure that its staff members receive adequate training to facilitate the identification of suspicious activity and adhere to the relevant reporting requirements.

i. clear transaction monitoring rules to aid in detecting unusual and suspicious activities/transactions

ii. requirements for continuous reviews of customer transactions for unusual patterns or red flags they should include setting triggers for specific transaction amounts and frequency,

iii. baseline requirements for customer profiles to make it easier to recognize deviations from normal behaviour

iv. establish clear reporting channels and frequency for internal staff reporting and reporting to the management and board

v. incorporate requirements for generating timely reports, escalation and subsequent case management.

vi. ensure processes are seamlessly integrated into work procedures and system requirements

**REVIEWS**

Section 20 (4) (a) of the Regulations, provides that service providers shall maintain adequate policies and procedures for monitoring and testing the effectiveness of: policies and procedures, including CDD and ongoing monitoring procedures. As such, service providers are mandated to conduct such reviews having regard to the guidance outlined on page 148, paragraph 25 (3) of the AML/CFT code, 2017.

***Conducting Internal and External Audits:***

Regular internal and external reviews/audits are important to ensure that the process of ongoing monitoring remains adequate and effective.

Review/audit of a service provider's systems policies, procedures, and controls relating to its AML/CFT ongoing monitoring must be performed by an individual(s) who is/are professionally competent, qualified, and skilled, and must be independent of:

- the function being reviewed;

- the division, department, unit, or other part of the entity where the function is performed; and

- external professionals must be independent of the process being audited, i.e., they should not have contributed to the design of the system.

## TRAINING

The continuous professional development of relevant staff and adoption of a systematic approach to AML/CFT/PF training is essential for maintaining effective and efficient ongoing monitoring systems. As such, service providers should provide regular training to employees, as it keeps staff updated on regulations, tools, and techniques required for detecting and responding to emerging risks and are sufficiently capable and skilled to operate the systems used for ongoing monitoring.

A service provider's training programme should also include regular and specific training for the Board and Committees to ensure they understand their roles and responsibilities and are sufficiently capable and skilled to provide effective oversight on an ongoing basis. Staff training needs should be assessed and addressed at least annually.

## COMMENCEMENT

These Guidelines shall come into effect this **1st day of September 2025**

**Issued by**:

Financial Services Authority
P.O. Box 356
Kingstown
St. Vincent & the Grenadines
Tel (784) 456-2577
Fax (784) 457-2568
Email: info@svgfsa.com