

Guide to How an Effective Ongoing Monitoring System Aids in Producing Quality Suspicious Activity Reports (SARs)

Suspicious activities include acts that give rise to a misgiving that a person (i.e. legal person, legal arrangement or individual) is attempting to hide/disguise the true nature of their activities or carry out a questionable transaction and may indicate potential abuse of the financial services regime.

A Suspicious Activity Report (SAR) is a tool used by Financial Institutions (FIs) and Designated Non-financial Businesses and Professionals (DNFBPs) to aid in detecting and reporting possible financial crimes. Once reported, SARs are then analysed by financial intelligence units (the Financial Investigative Agency (FIA) in the case of the VI) to determine whether the suspicious activity reported warrants further investigation by law enforcement agencies such as the Royal Virgin Islands Police Force (RVIPF). Financial institutions' assessment and filing of SARs are, therefore, integral elements in forestalling illicit activities.

The quality of the information provided in a SAR filed with the FIA is critical in ensuring that the FIA is able to properly analyse the information submitted and make an informed decision as to whether the reported activity warrants further investigation by the RVIPF and/or another local or foreign law enforcement agency.

To recognise suspicious activities, entities should, amongst other requirements under the VI's AML/CFT regime, ensure that they:

- conduct proper customer risk assessments in order to know their customers;
- monitor their customer's behaviour and transaction history; and
- ask appropriate questions when activities appear out of the ordinary.

Having robust ongoing monitoring processes and procedures in place is a critical component for entities in identifying business activities and transaction patterns that may be inconsistent with their customers' profiles, and which may signal potential suspicious activity. This is particularly important where the risk associated with the client relationship is already elevated. Ongoing monitoring also aids in identifying when a client's circumstances change (e.g. becoming sanctioned or named in some criminal activity), which may require a SAR to be filed with the FIA or trigger the updating of the client's risk profile. Being able to identify such behaviour and properly document it is another key component in producing a quality SAR.

Sufficient information on the activity or transaction should be collected to determine whether the activity/transaction can be explained. Where it cannot be explained and it is determined that a SAR should be filed, as much detail as possible on the suspected activity/transaction should be included in the SAR. The FIA's *Suspicious Activity/Suspicious Transaction Checklist* and *Instructions Regarding the Revised STR Form* should be used as a guide to determine what information should be included in the SAR. These documents can be found [here](#) on the FIA's website.

A quality SAR should include the 5Ws (Who, What, Where, When, Why) and 1H (How) and should thoroughly describe the suspicion being reported, along with the relevant factors that raised the suspicion. All SARs should include, *inter alia*:

- the name and contact details of the person filing the report;
- details of the person(s) involved of the suspicious activity/transaction, including source of funds and source of wealth;

- a detailed summary of the identified activity/transaction including, where applicable:
 - where and when the activity/transaction occurred and how it was detected,
 - names and background information of persons involved,
 - any patterns or behaviors observed over time to support suspicion,
 - description and value of assets/transactions involved (assets include but are not limited to real estate, investment accounts, shareholdings in other companies, sea vessels, and foreign or domestic bank accounts);
- rationale for the suspicion;
- whether the activity relates to money laundering or any of its predicate offences, terrorist financing, proliferation financing or other illicit activity;
- whether or not the SAR has been filed with any other jurisdiction and if so, the name(s) of the jurisdiction(s); and
- any supporting documents that could help to support the suspicion (e.g. bank statements, invoices, receipts etc.).

Relevant entities should also refer to the Commission's *Guidance - An Effective Approach to Ongoing Monitoring*, which includes warning signs and red flags that may emanate from transaction monitoring activities, for information on how to carry out proper monitoring.

Additional information on indicators that may identify suspicious activity can be found in the Explanatory Notes of section 21 of the AML Code of Practice.

Higher Risk Sectors: Examples of Information that can enhance the Quality of SARs

In relation to higher risk sectors such as the Trust and Corporate Services Providers (TCSPs), Virtual Asset Services Providers (VASPs) and Investment Business sectors, information that could enhance the quality of SARs filed may include: (note that where relevant, some identified issues are appropriate for all sectors)

VASPs	TCSPs	Investment Businesses
Accurate date and time of suspicious transaction, including accurate dates in ledger reports as this allows for effective correlation with blockchain data	Information on ownership and control, which includes shareholder structure, persons who have the right to appoint or remove majority directors, de facto control, control via voting rights, and contractual agreements	Details of the product or service offered to the customer - features of the product should include investment method (cash, cheque, wire, etc.), investment terms (tenure, interest rate, etc.)
Wallet addresses and Type - All wallet addresses involved should be disclosed, along with an indication of the wallet type (e.g., hot wallet, cold wallet, multi-signature wallet, or customer's	Information on networks concerning the subject(s) of the SAR, which includes whether the subject is or is associated with a PEP, or any known criminal organisations, foreign or domestic.	Where funds are held in trust or for a third party, the KYC information for all such individuals should be included in the SAR, (e.g. full/registered name, date of birth, identification

personal wallet). This helps the FIA gain a better understanding of the activity to investigate it effectively		document type and number, address (residential and otherwise), nationality etc.).
Transaction hashes associated with the suspicious activity should be provided	Information on any sanctioned BOs who may have attempted to make a change in the ownership structure of the company prior to designation	Source of funds for each investment - if the funds for investment are provided by a third party, KYC documentation should be provided for that individual/entity, (e.g. full/registered name, date of birth, identification document type and number, address (residential or otherwise), nationality etc.). Source of wealth for the client including documentation/evidence
Any external intelligence that supports the suspicion (e.g. OFSI designations and blockchain analytics reports and any reports which may link addresses to sanctioned or other high-risk entities/individual).	Any external intelligence that supports the suspicion (e.g. OFSI designations and any reports which may link to sanctioned or other high-risk entities/individual)	Any external intelligence that supports the suspicion (e.g. OFSI designations and any reports which may link to sanctioned or other high-risk entities/individual)
		Location of where invested fund are being held
		Information on expected and actual level of activity on the account

Regulated entities are encouraged to be diligent in the application of their AML/CFT/CPF measures, ensure staff are trained to effectively fulfil their monitoring obligations, and ensure they are able to properly document identified suspicious activity. This will aid in enhancing the quality of SARs filed with the FIA and further assist law enforcement in successfully investigating and prosecuting any identified criminal activity.

Both the FSC and the FIA will continue to actively engage entities, including through onsite inspections and desk-based reviews, to assess compliance with their SARs obligations, including assessment of the quality of SARs submitted. Regulated entities should therefore review their controls, policies and procedures and carry out an assessment of the quality of SARs submitted to ensure compliance with the requirement related to SARs.