GIBRALTAR FINANCIAL SERVICES COMMISSION

8. Policies, Procedures & Controls

GFSC AML/CFT/CPF Guidance Notes

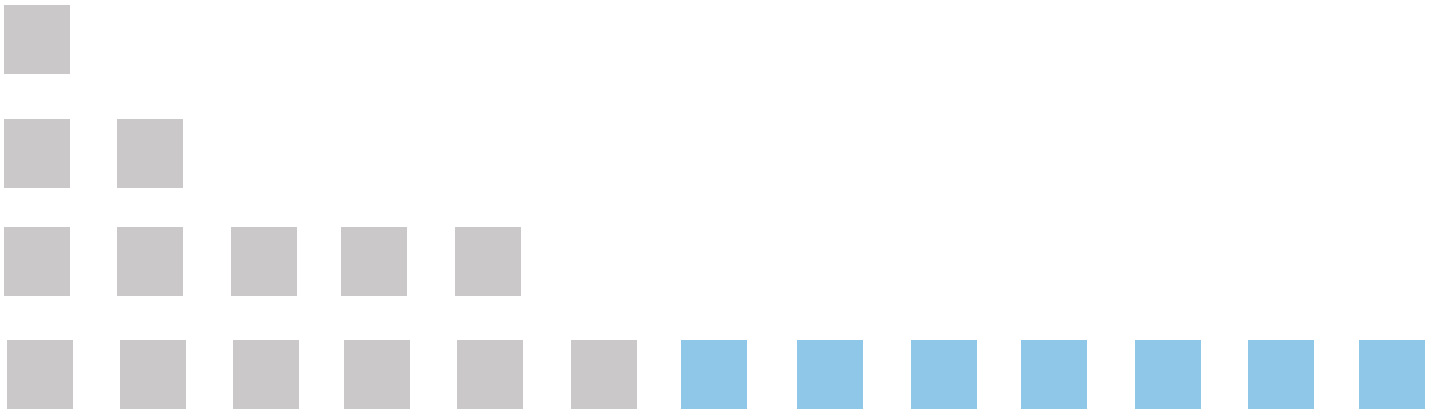

Table of Contents

8.1 Establishment and Maintenance of Policies and Procedures

AML/CFT/CPF Requirements

R23 A regulated entity must establish and maintain appropriate and adequate risk-sensitive policies, controls and procedures. Such policies, controls and procedures must be proportionate to the nature and size of the regulated entity's business. A regulated entity will be responsible for establishing, implementing and maintaining these, including enhancing these where higher risks have been identified.

Guidance

1. A regulated entity's policies, controls and procedures must be adequate, appropriate, and effective in preventing and detecting ML, TF, and PF. A regulated entity must therefore establish, implement and maintain appropriate and risk sensitive policies, controls and procedures relating to[1]:
    a. Customer due diligence measures and ongoing monitoring;
    b. Reporting;
    c. Record-keeping;
    d. Internal control;
    e. Risk assessment and management;
    f. Compliance management and appointment of responsibility for the establishment and maintenance of effective systems of control to a compliance officer at management level (being a director, senior manager or partner); and
    g. Employee screening.

2. The policies, controls and procedures mentioned above must be appropriately aligned with the nature and scale of the business[2]. This indicates that a regulated entity must ensure that its policies and procedures are tailored to match the type of business it conducts, the services it provides and the inherent risks involved. In cases where policies and procedures are developed and drafted by a third-party, these factors should be taken into account as these tend to be overly generic, lacking specificity and may not cater to the unique activities of the regulated entity.

3. A regulated entity must ensure it monitors the application and implementation of those policies, controls, and procedures, including enhancing these where it has identified areas of higher risk[3].

4. A regulated entity is responsible for ensuring that its policies and procedures are reviewed on an ongoing basis and updated when there are any changes made to legislation or relevant guidance.

5. The policies, controls and procedures referred to above also include those that relate to the identification of complex or unusually large transactions, unusual patterns of transactions which have no apparent economic or visible lawful purpose and any other activity which the regulated entity regards as related to ML, TF, or PF[4] by nature.

[1] Section 26(1), Proceeds of Crime Act 2015
[2] Section 26(1ZA), Proceeds of Crime Act 2015
[3] Section 26(1ZB), Proceeds of Crime Act 2015
[4] Section 26(2)(a), Proceeds of Crime Act 2015

6. The policies, controls and procedures must also specify the additional measures taken, where appropriate, to prevent the use of products and transactions which may favour anonymity increased the ML, TF or PF risk[5].

7. Additionally, a regulated entity should establish procedures which help employees determine whether a customer or a beneficial owner of a customer is a politically exposed person, family member or close associate of a PEP[6].

8. It is essential that all directors, senior managers, MLROs and employees within a regulated entity be fully acquainted with and understand the regulated entity's policies and procedures, particularly when such policies and procedures have been prepared by a third-party.

8.2 Independent Audit

AML/CFT Requirements

R24 A regulated entity is required to undertake an independent audit in order to assess its AML/CFT/CPF policies, procedures and controls in ensuring compliance with the requirements listed under Section 26(1) of the Act. The independent audit must have regard to the size and nature of the business which will determine the frequency and scope of the assessment.

Guidance

9. A regulated entity must undertake an independent audit function for the purposes of testing the policies, controls, and procedures as stated in 8.1, and which has regard to the size and nature of the business[7].

10. The frequency and scope of the independent audit function is to be determined by the regulated entity applying a risk-based approach in line with the size and nature of its business. This should be considered on an ongoing basis.

11. The independent audit function should be performed by individual(s) who are operationally separate from the regulated entity's compliance function. It is the ultimate responsibility of a regulated entity to ensure the independence of those performing this function. The independent audit may be performed by an individual within the firm or externally, having regard to the independence of the role.

12. It is the responsibility of a regulated entity's senior management to monitor and review the effectiveness of its independent audit function and ensure that any outcomes, findings or deficiencies identified are addressed accordingly.

13. A regulated entity may demonstrate that it has tested the effectiveness of its policies, procedures and controls by producing periodical reports which show that compliance with its policies and procedures is being monitored. The reports should highlight any deficiencies that have been identified in light of the independent review, as well as any details of actions taken by the regulated entity in demonstrating its commitment to address these shortcomings.

[5] Section 26(2)(b), Proceeds of Crime Act 2015
[6] Section 26(2)(c), Proceeds of Crime 2015
[7] Section 26(1A), Proceeds of Crime Act 2015

8.3 Powers to Require Information and Production of Policies and Procedures Documentation

14. Each regulated entity has a duty to make its policies and procedures available to the GFSC as and when required in accordance with Regulation 12(1) of the SBPR.

8.4 Branches or Subsidiaries

15. If a regulated entity has branches or subsidiaries, it is required to implement group-wide policies and procedures that apply to all its branches and majority-owned subsidiaries within its group which must, as a minimum, meet Gibraltar standards and requirements.
These should include the following[8]:
    a. Policies, controls and procedures, as those mentioned in 8.1;
    b. Policies and procedures for sharing information required for the purposes of satisfying the customer due diligence requirements within the group;
    c. The provision, at group-level functions, of customer, account and transaction information from branches and subsidiaries, where necessary, for the purposes of AML, CFT and CPF, which shall include, to the extent permitted under the Data Protection Act 2004 –
        i. Information about transactions or activities which appear unusual; and
        ii. Any analysis carried out in respect of transaction or activities which appear suspicious, including the content of any report made to the GFIU or the underlying information where such disclosure is made in confidence and would not cause tipping-off of the customer.
    d. Adequate safeguards on the confidentiality and use of the information exchanged under customer due diligence requirements, including safeguards to prevent tipping-off; and
    e. The provision of information from group-level functions to branches and subsidiaries where relevant and appropriate to the management of the risks of ML, TF and PF.

16. The "group-level" functions referred to above, relate to any functions concerning compliance, audit or AML/CFT/CPF controls[9].

8.5 Systems and Controls

17. A regulated entity must have systems and controls in place to be able to identify, assess, monitor and manage ML, TF, and PF risks. These controls must be proportionate to the nature, size and complexity of the regulated entity's business and activities.

18. A Regulated entity is required to regularly assess its systems and controls in order to ensure that it continues to comply with the requirements under the Act.

19. When implementing systems and controls to detect and prevent financial crime, a regulated entity needs to identify the ML, TF, and PF risks which it may be exposed to by considering its customers, distribution channels and the volume and complexity of its transactions. A regulated entity should therefore ensure that it has systems and controls in place which covers all these areas, including those mentioned under Section 26 of the Act.

20. In order for a regulated entity to establish and maintain appropriate and effective systems and controls, it must:

[8] Section 26(1B), Proceeds of Crime Act 2015
[9] Section 26(1BB), Proceeds of Crime Act 2015

- Ensure that appropriate provision of information is provided to senior management, including, as a minimum, an annual report by the regulated entity's MLRO on the operation and effectiveness of its systems and controls;
- Implement adequate training plans for employees on ML, TF, and PF and ensure that relevant staff are kept informed of domestic legislation/requirements as well as any relevant guidance issued relating to AML/CFT/CPF;
- Maintain appropriate documentation on the regulated entity's risk management policies and risk profile in relation to ML, TF and PF including, documentation of its application of those policies;
- Apply measures which ensure that ML, TF and PF risks are taken into account in the daily operations of the business, including the development of new products, the onboarding of customers and any changes to the business model;
- Establish a policy and procedure for conducting sanctions screening on all potential and existing customers to ensure compliance with Section 8(3) of the Sanctions Act 2019. This entails conducting ongoing screening of customers (including officers and beneficial owners) against the relevant sanctions lists to ensure they are not individuals or entities subject to designation/sanctions[10];
- Keep documents, data and information on customers up-to-date including any changes in beneficial ownership and/or control;
- Establish a policy and procedure for employee screening and adequately screen all employees prior to the commencement of their employment;
- Ensure that reports are made to the GFIU when it is known, suspected, or there are reasonable grounds to know or suspect, that another person is involved in ML, TF or PF and ensure that the process for disclosures, is included in the regulated entity's policies and procedures document;
- Make certain that its policies and procedures document is readily accessible and made available to all staff members, particularly for those policies and procedures that are relevant to an employee's role;
- Maintain appropriate and consistent policies and procedures which provide for the ongoing monitoring of transactions and customer activity;
- Share policies and procedures with its branches or subsidiaries and monitor their compliance;
- Maintain complete records and implement adequate record-keeping procedures so documents can easily be accessed on a timely basis if requested by the GFSC or another relevant authority.

21. The level of systems and controls that a regulated entity implements and the extent to which monitoring needs to take place, is determined on the regulated entity's size, the complexity of its operations, the services it provides, the type of business transactions it is involved in and its overall risk profile.

22. The regulated entity must appoint an AML/CFT Director to oversee all AML/CFT/CPF systems and controls and to ensure that they have been effectively implemented. For further information, please refer to the "Responsibility of Key" Individuals section within these Guidance Notes.

8.6 Outsourcing Systems and Controls

AML/CFT Requirements

[10] Section 10(ca), Proceeds of Crime Act 2015

R25 In cases where a regulated entity has chosen to outsource certain systems and controls, it is required to retain adequate oversight of and responsibility for such outsourced arrangements.

Guidance

23. When a regulated entity chooses to outsource its systems and controls, wholly or partly, it must ensure that this decision does not lead to reduced standards of compliance. A regulated entity can outsource a function, but it is not absolved of its responsibility for compliance and will remain ultimately liable for all systems and controls implemented, regardless of the outsourcing arrangement in place[11].

24. It is the responsibility of a regulated entity to ensure that any third-party provider maintains appropriate and satisfactory AML, CFT and CPF systems and controls on its behalf. The regulated entity must also ensure that the relevant policies, controls and procedures remain up-to-date and align with any changes to domestic legislation, as well as, any appropriate guidance issued.

25. If a regulated entity has decided to outsource its systems and controls, wholly or partly, its policies, procedures, systems, and controls should include when outsourcing will be permitted, and under what conditions.

For further guidance on outsourcing arrangements, please refer to the GFSC's Outsourcing Guidance Note[12]. A regulated entity is required to ensure compliance with outsourcing requirements under the Act, these Guidance Notes as well as the Outsourcing Guidance Notes.

8.7 Sanctions Screening

AML/CFT Requirements

R26 A regulated entity is required to conduct appropriate sanctions screening on all customers and their beneficial owners:

a) Prior to establishing a business relationship or an occasional transaction; and
b) On an ongoing basis, in line with the updates to the relevant sanctions lists.

Guidance

26. As part of a regulated entity's customer due diligence obligations, the Act requires a regulated entity to conduct sanctions screening[13].

27. A regulated entity is therefore required to carry out sanctions screening of all business relationships and occasional transactions. This screening must include the customer, any beneficial owners and/or controllers and other associated parties.

28. The screening must be carried out at the start of a business relationship as well as on an ongoing basis. The screening must be carried out without delay whenever there is an amendment or change made to the required sanctions lists.

29. The Sanctions Act 2019 provides for the automatic recognition and enforcement of UN, UK, and EU sanctions to which a regulated entity is subject to when conducting its sanctions screening. The Sanctions Act 2019 and the Terrorist-Asset Freezing Regulations 2011 also provide for separate Gibraltar sanctions designations to be made by the relevant competent authority in Gibraltar.

[11] Section 23(4), Proceeds of Crime Act 2015
[12] https://www.fsc.gi/uploads/legacy/download/adobe/GuidanceNote-Outsourcing.pdf
[13] Section 10(ca), Proceeds of Crime Act 2015

30. A regulated entity is subject to the enforcement of UN, EU, UK & Gibraltar sanctions[14] and should ensure that it maintains awareness of any additional targets that have been designated locally under the Sanctions Act 2019 or the Terrorist Asset-Freezing Regulations 2011.

31. The restrictive measures imposed by the UK will always take precedence in circumstances where restrictive measures have been imposed by both the UK and EU[15].

32. In determining the suitability of automated versus manual screening, a regulated entity should assess various factors, including: its respective sector; the frequency of updates to relevant lists; the number of customers on the client base; the resources available including capacity of staff; and the volume and complexity of transactions. If a regulated entity chooses to implement an automated screening system, it must ensure that any sanctions monitoring arrangements with third party providers have been adequately assessed and are deemed to comply with the local legislative requirements.

33. As stated within the "Suspicious Activity Reporting" section of these Guidance Notes, all MLROs must register an account with Themis in order to receive notification of sanctions notices from the GFIU via the Themis Notice Board.

34. For further information on local designations and sanctions measures please visit the GFIU website and the GFIU's Financial Sanctions Guidance Notes.

Sector-specific Guidance – Virtual Asset Service Providers ("VASPs")

35. A regulated entity operating as a VASP (either as an authorised DLT Provider or registered VASP) must implement virtual asset screening controls in order to identify any association between its customer wallet addresses and potential illicit activity.

36. Virtual asset wallet addresses may be subject to financial sanctions in the same way as individuals and legal entities. When engaging with the wallet address of a customer, a regulated entity must therefore ensure to screen the respective wallet address to ensure that it is not subject to any relevant designations.

[14] Section 6(2), Sanctions Act 2019
[15] Section 6(3), Sanctions Act 2019

GIBRALTAR FINANCIAL SERVICES COMMISSION

Published by:
Gibraltar Financial Services Commission
PO Box 940
Suite 3, Ground Floor
Atlantic Suites
Europort Avenue
Gibraltar

www.gfsc.gi