GIBRALTAR FINANCIAL SERVICES COMMISSION

4. Customer Risk Assessment

GFSC AML/CFT/CPF Guidance Notes

Table of Contents

4.1 Application of a Risk-Based Approach

AML/CFT CPF Requirements

R9 Prior to the inception of a business relationship or occasional transaction, a regulated entity must assess the ML, TF and PF related risks posed by each customer. This assessment must take into account customer, country, product and interface risk factors.

R10 The risk assessment undertaken for each customer must be refreshed periodically throughout the business relationship to ensure that it remains an appropriate and relevant reflection of the ML, TF & PF risks posed by the business relationship.

Guidance

1. In accordance with the Act, a regulated entity must take appropriate steps to identify the ML, TF and PF risks faced by its business operations, taking into account risk factors relating to each of its customers[1]. In practice, the ML, TF & PF risks to which each regulated entity is exposed to differs as a result of a multitude of factors, including the specific customer that the regulated entity is engaging with in that instance. A regulated entity must therefore develop a robust understanding of the risk profile of each prospective business relationship and occasional transaction prior to its inception, in order to determine the level and intensity of mitigating measures and controls that are required to satisfactorily address the risks posed. The development of a risk-based approach allows for a proportionate application of these measures that is commensurate to the level of risk posed by that client/relationship.

2. When assessing the risk profile of a prospective customer, the following risk factors must be taken into consideration:
    a) Customer risk;
    b) Product risk;
    c) Country risk; and
    d) Interface risk.

3. Together, all four risk elements outlined above must be considered in unison in order to produce an overall risk profile. It is the result of this risk profile that will then determine the level and intensity of the identification, verification and monitoring measures applicable to that business relationship.

4.2 Customer Risk

4. Customer risk refers to the risks posed by a specific customer based on their nature, characteristics, behaviour, reputation and economic activity. The circumstances surrounding a customer will vary the ultimate threat or vulnerability of the customer being involved in ML, TF, PF or other types of illicit activities. The intensity of the identification, verification and monitoring measures applied to the customer must therefore increase with the perceived or potential threat posed. Please refer to the sections in this Guidance Note on Customer Due Diligence for further guidance on establishing and implementing these measures.

5. In formulating its strategy and business plan, a regulated entity should develop a view of the specific types of customers that it intends on engaging with by means of its product offering.

[1] Section 25A, Proceeds of Crime Act 2015

This should include an assessment of the types of customers that would fall outside of its risk appetite as a result of the ML, TF & PF risks posed.

4.2.1 Individuals

6. The variation in risk posed by different individuals is predominantly as a result of their economic activity, including the means through which they have generated their income and wealth. These factors must be formally considered when classifying the customer risk posed by a business relationship.

7. When assessing customer risk, a regulated entity must take into account the underlying economic activities through which the customer's income and wealth have been generated. The risk posed by a salaried individual, for example, may differ dependent on the nature of business of their employer (e.g. in the case where the employer's business is cash intensive, or is associated with high risk jurisdictions). As part of a regulated entity's assessment of a customer's nature and behaviour, it must also consider the presence of any relevant adverse media on an individual or entity, or any other relevant sources of information.

8. Through the application of identification measures, a regulated entity has an obligation to identify any parties subject to designations, such as known or suspected terrorists, or individuals and entities which have been the subject of sanctions or other economic measures. Irrespective of the perceived level of risk posed through the assessment of other risk factors, a sanctioned/designated customer should usually result in the mandatory declining or cessation of the business relationship and would trigger a requirement for the regulated entity to inform the relevant authorities of the sanctioned individuals/entities.

9. Depending on the nature of products and services being offered by the regulated entity, additional factors, such as the age of the customer, may also be indicative of potential increased risk. This is particularly relevant where the customer is in a vulnerable age bracket and may therefore be susceptible to various types of fraud.

4.2.2 Legal Entities and Arrangements

10. Legal entities including companies, trusts, foundations and partnerships are recognised internationally as vehicles through which opacity in financial transactions can be easily introduced. These entities are often used by criminals to introduce layers of separation between the illicit activity being conducted and those individuals who are ultimately deriving the benefit.

11. In all cases, a regulated entity is required to appropriately identify and verify the ultimate beneficial owner(s) of clients that are corporates. As the complexity of a corporate structure increases, so does the potential opacity surrounding beneficial ownership and, as a result, the level of risk posed. Although the introduction of factors which add to the complexity of corporate structures (such as nominee shareholding, declarations of trust and powers of attorney) have legitimate use cases, a regulated entity must recognise the risks associated with these and have appropriate controls in place to ensure that these are properly mitigated.

12. Different types of legal entities present different levels and types of threats relating to ML, TF and PF. The underlying activity of each entity (including that of each of the ultimate beneficial owner(s)) will also vary and must be considered as part of the assessment (e.g. if it is a trading company, asset holding company, shipping company, etc.).

13. In practice, legal entities are run and operated by their shareholders, beneficial owners, officers and managers (or any other equivalent individuals exercising control over the legal entity, legal

arrangement or similar). An assessment of these key individuals must therefore be reflected within the risk profile of the client entity.

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

14. When processing deposits and withdrawals of virtual assets to/from a customer's personal wallet address, VASPs are required to apply virtual asset screening measures to identify any potential direct or indirect exposure to known illicit sources. In cases where exposure is identified and is assessed to be relevant to the business relationship, the risk posed by that exposure should be factored into the customer's overall risk profile (as a customer risk factor) and may therefore warrant the application of additional mitigating measures. Depending on the nature of the exposure, this may warrant the declining or cessation of the business relationship, as well as the disclosure of a SAR to the Gibraltar Financial Intelligence Unit.

4.3 Product Risk

Guidance

15. Product risk refers to the risk associated with the nature of products and services being provided by the regulated entity in question. Different products and services will present different threats and vulnerabilities in potentially being used to facilitate ML, TF and PF. As a result, some services may appear inherently more attractive to criminals than others.

16. The development and publication of the HM Government of Gibraltar National Risk Assessment is the process through which Gibraltar seeks to identify these threats and vulnerabilities. This document sets out the risks associated with each of the potential products and services provided by the sectors regulated by the GFSC and should be used as the foundation for a regulated entity's assessment. Ultimately, it is the responsibility of the regulated entity to have a robust understanding of the risks posed by its business operations, so that it is then effectively able to implement the controls necessary to mitigate them. For more details on carrying out a Business Risk Assessment, please refer to the relevant section within these Guidance Notes.

17. In cases where a regulated entity offers multiple products and services, it is important to note that the risk posed by each respective service should be considered separately. When risk profiling a business relationship, the risk assessment should be specific to the exact product offering that the relevant client is seeking.

Example – Trust & Company Service Provider

18. A Trust & Company Service Provider (TCSP) may offer a range of services within the scope of its permission. These may include providing:
    - Directorship services;
    - Trusteeship services;
    - Foundation councillorship services;
    - Nominee shareholding services;
    - Secretarial services; and
    - Registered office services.

19. Ultimately, each of the specific services outlined above are subject to different types and levels of threats and vulnerabilities which could potentially be exploited by criminals. As an example, the HM Government of Gibraltar National Risk Assessment identifies the provision of nominee shareholding services as a potential means to allow for the concealment or obfuscation of

beneficial ownership. While threats and vulnerabilities exist in relation to each of the services identified above, the level of risk present is likely to vary in accordance with:

a) The nature of the customer being engaged;
b) The jurisdictions involved in the provision of the product/service; and
c) The channels through which the product/service is being delivered.

4.4 Country Risk

AML/CFT/CPF Requirements

R11 A regulated entity must apply enhanced due diligence and ongoing monitoring measures to customers established in high risk jurisdictions.

Guidance

20. Country risk refers to the risk posed by the geographic location of the economic activity associated with the business relationship. In addition to the country of residence/establishment of the customer and beneficial owner(s), the assessment must also include the jurisdictions through which economic activity of the customer and beneficial owner(s) has been derived and associated with.

21. In accordance with the Act, a regulated entity is required to apply enhanced due diligence and ongoing monitoring measures in cases where a customer is established within a high risk jurisdiction[2]. This is regardless of the overall scoring of the other risk factors taken into consideration within the customer's risk profile, where these in aggregate result in a low or medium risk score that would not otherwise warrant an enhanced approach.

4.4.1 Assessing Countries & Territories

22. In order to quantify the country risk posed by prospective business relationships, a regulated entity must assess and document the risk posed by different jurisdictions and territories. In doing so, the regulated entity must pay due regard to the effectiveness of that jurisdiction's legislative, regulatory and operational measures in combatting ML, TF & PF.

23. The onus is ultimately on the regulated entity to determine the level of risk posed by each jurisdiction. The methodology through which this assessment is undertaken, is also ultimately up to the discretion of each regulated entity and needs to be in line with the regulated entity's risk appetite. In practice, when conducting such assessments, a regulated entity is able to rely on reputable sources of information, including internationally accepted lists. In making a determination on the effectiveness of a jurisdiction's AML/CFT/CPF regime, the following factors must be taken into consideration:

a) The jurisdiction's AML/CFT/CPF legal framework;
b) The jurisdiction's AML/CFT/CPF supervision and enforcement regimes; and
c) The jurisdiction's ability to cooperate with authorities internationally.

24. The FATF publishes two lists identifying jurisdictions with weaknesses or deficiencies in their AML/CFT/CPF regimes, in-keeping with the above-mentioned factors. The first is a list of "high risk jurisdictions subject to a call for action". This list identifies countries and territories with significant strategic deficiencies in their measures to counter ML, TF & PF. For all jurisdictions listed, the FATF urges the application of enhanced due diligence, and, in the most serious cases, the application of counter-measures to protect the international financial system from the ML,

[2] Section 17(1)(b), Proceeds of Crime Act 2015

TF & PF risks emanating from the country. The list is often externally referred to as the "black list".

25. The second list published by the FATF is in relation to "jurisdictions under increased monitoring". These jurisdictions are actively working with the FATF to address the deficiencies identified within their AML/CFT/CPF regimes identified through a mutual evaluation. In this case, the FATF calls for a risk based approach to these jurisdictions and encourages its members to take into account the information presented on each jurisdiction within their risk assessments. This list is often externally referred to as the "grey list".

26. In addition to the FATF lists referenced above, the United Kingdom and European Union have both published lists of countries and territories deemed "high risk third countries" as a result of strategic deficiencies identified within their AML/CFT/CPF regimes.

4.4.2 Conflict Zones

27. The term "conflict zone" refers to a geographic region whose security is compromised as a result of active, or likely armed, conflict between two or more militarised parties. This extends to regions with established links to active terrorist organisations, including such cases where:

a) Terrorist organisation(s) are established and active within the jurisdiction;
b) The jurisdiction is neighbouring, or shares a border with, a territory or region controlled by a terrorist organisation;
c) The jurisdiction is used for the generation of funds and assets on behalf of terrorist organisation(s); and
d) The jurisdiction is considered an active transit point for the movement of funds or goods on behalf of terrorist organisation(s).

28. As a result of the presence of armed conflict, the establishment and facilitation of business relationships or transactions with such jurisdictions presents an increased level of TF risk. This should therefore be considered within the regulated entity's country risk scoring methodology. To aid in the identification of current conflict zones, a regulated entity may rely on publicly available information, such as the Global Conflict Tracker published by the Council on Foreign Relations[3].

4.4.3 Drug Producing & Transiting Jurisdictions

29. The United States Department of State periodically publishes a report identifying the jurisdictions which are known as major territories in the development and transit of illicit drugs[4]. The report is not intended to be a reflection of each jurisdiction's preventative controls, law enforcement measures or international cooperation relating to the production and movement of narcotics. The listing of a jurisdiction within the report is instead cited as a result of a combination of geographic, commercial and economic factors which have led to the establishment of drug production and transit systems.

30. The link between drug production and distribution activities and the economic activity of such jurisdictions presents an increased level of ML risk. When dealing with such jurisdictions, a regulated entity is therefore required to determine whether any additional mitigatory measures should be put in place to counteract the ML risks posed.

[3] Council on Foreign Relations Global Conflict Tracker

[4] U.S. DOS International Narcotics Control Strategy Report

4.4.4 Jurisdictions with a Propensity for Bribery & Corruption

31. The corruption of public officials within any given jurisdiction is known to be intrinsically linked to ML, TF or PF. As with other criminal activities, corruption-related offences (such as bribery and the theft of public funds) are generally committed for the purposes of private gain.

32. The controls in place to prevent the susceptibility of a jurisdiction's financial system to corruption vary depending on the jurisdiction in question. The level of risk posed is particularly heightened in cases where the business relationship in question is held with a Politically Exposed Person (or a known close associate or family member of a PEP) holding a prominent public function within a jurisdiction identified as having a propensity for corruption.

33. In order to assess the level of corruption associated with a given jurisdiction, a regulated entity may rely on publicly available information and lists, such as the Corruptions Perception Index published by Transparency International[5].

4.4.5 Sanctioned Countries & Territories

34. As with entities and individuals, countries and territories may also be subjected to sanctions and other economic measures. These may require entities to take action to prohibit:
    a) The export of goods to those countries or territories;
    b) The transfer of technology and/or resources;
    c) The facilitation of technical assistance; and
    d) The facilitation and transfer of funds.

35. As set out under the Sanctions Act 2019, the following sanctions regimes apply within Gibraltar:
    - United Nations;
    - European Union;
    - United Kingdom; and
    - Gibraltar.

36. The Terrorist-Asset Freezing Regulations 2011 transposes the following council resolutions into local legislation:
    - United Nationals Security Council Resolutions 1373, 1452, and successor resolutions; and
    - EU Council Regulation 2580.

37. As a result of these economic measures, it is likely that a regulated entity will be required to freeze assets related to designated undertakings and/or individuals in these circumstances. In addition, the regulated entity may need to decline or cease the business relationship and report the matter to the relevant authorities. Further guidance on the application of sanctions measures can be found within the "Policies, Procedures & Controls" section of these Guidance Notes.

4.4.6 High Risk NRA Countries

38. The NRA includes an assessment of the jurisdictions which are considered to pose an increased threat to Gibraltar as a result of Gibraltar's geographic location. The first of the jurisdictions identified is Spain. In respect of Spain, the NRA highlights "the proximity to OCG's as one of the primary risks that could potentially impact Gibraltar" given it may lead to ML.

[5] Transparency International Corruption Perceptions Index

39. In much the same way that physical proximity is identified as a key factor in assessing the risk posed by Spain, Morocco is also identified within the NRA as a jurisdiction of increased risk. In the case of Morocco, the risk set out within the NRA is predominantly associated with the level of cannabis production identified within the jurisdiction which would lead to a high level of drug producing/trafficking and ML as a result.

40. The threats, vulnerabilities and risks identified within the NRA must be taken into account by a regulated entity when conducting both business and customer risk assessments. In doing so, a regulated entity is able to document any mitigating measures and controls which have been implemented to mitigate the specific risks identified. In practice, the NRA calls for the consideration and categorization of funds received from either Spain or Morocco as high risk (and are therefore required to be subjected to additional controls in accordance with each entity's risk-based approach).

4.5 Interface Risk

41. Interface risk refers to the risk resulting from the mechanism through which the business relationship is commenced and transacted.

4.5.1 Face-to-face vs. Non-face-to-face Interactions

42. It is recognised that where a regulated entity makes face-to-face contact with a customer, this is perceived to lower the interface risk associated with that business relationship. This is on the basis that the entity has been able to verify the likeness of the individual against the submitted identity documentation.

43. For the purposes of these Guidance Notes, video calls conducted over the internet are also considered to be equivalent to a face-to-face interaction. A regulated entity must ensure, however, that the video call in question is conducted in a secure environment to prevent the individual from altering or tampering with their appearance.

44. Any mechanism through which the customer is allowed to interact with a regulated entity in a non-direct manner increases the entity's exposure to interface risk. In such cases, a regulated entity is required to establish and maintain adequate measures to appropriately address and mitigate the risk posed. Examples of such identity verification measures may include:
    a) Requesting additional documents, data or information from the customer;
    b) Requiring the certification of the submitted identification documents;
    c) Ensuring that the first payment received from the customer is remitted from an account in the customer's name;
    d) Sending information or documents required to operate the business relationship to a physical address which has been verified; and
    e) Applying technological solutions which allow for the facial comparison between a "live selfie" of the customer and the submitted identification documents.

45. It is ultimately the responsibility of each regulated entity to determine which exact measures are to be applied in mitigating the level of interface risk posed by each prospective business relationship. When relying on the use of technological systems provided by third parties for the purposes of customer identity verification, a regulated entity should consider:
    a) The appropriateness of the parameters used to determine the authenticity of the submitted documentation/information;
    b) The appropriateness of the system in line with the regulated entity's size and nature of their business and the sector in which it operates;

c) The breadth, size and validity of data sources used;
d) Whether the identification documentation submitted in the jurisdictions within which the regulated entity seeks to engage in business are compatible with the selected tool; and
e) Whether the tool is able to adequately identify non-latin characters (where necessary).

4.5.2 Introducers & Intermediaries

46. Regardless of the method through which a customer is engaged, the ultimate responsibility for ensuring that customer identification measures are adequately met is retained by the regulated entity and its senior management.

47. A regulated entity must hold appropriate records in relation to the customer due diligence documentation received of its clients. This is regardless of whether the customer is referred to the regulated entity through a business associate or sister company.

48. There are certain circumstances in which it may be possible for a regulated entity to place reliance on the customer identification documentation collected by third parties. This is in the case of introduction via an eligible introducer. For further information on the definition and scope of eligible introducers, please refer to the "Customer Due Diligence" section of these Guidance Notes.

4.6 Mandatory High Risk Factors

49. It is important to note that there are several factors which would lead to a client being automatically scored as high risk, regardless of the scoring of other risk factors. These clients would be required to be subjected to enhanced due diligence and ongoing monitoring measures. These factors include:

- PEP status;
- Establishment in a high risk jurisdiction (as set out above); and
- Cases of increased ML, TF or PF risk (as identified by the regulated entity or Minister for Justice by notice in the Gibraltar Gazette).

50. A regulated entity may determine additional factors which are considered material and high risk to its own business, and which would automatically lead to a client being scored as high risk. This should be in line with its own risk tolerance levels and business risk assessment. A regulated entity may determine, for example, that a particular set of client activities may pose a higher level of risk which would in turn warrant that client being subject to enhanced due diligence and monitoring processes.

4.7 Conducting the Customer Risk Assessment

51. In order to ensure consistency and proportionate mitigation measures, a regulated entity should have a clearly documented customer risk assessment methodology. This methodology should be reviewed and updated on an ongoing basis to ensure that it remains accurate, current and captures all risks relevant to the operations of the business.

52. The method through which the risk assessment is conducted in practice is at the discretion of the regulated entity. In cases where a regulated entity intends on applying a numerical risk scoring system, due care and consideration must be paid to the weightings applied to each risk factor to enable an accurate end score. A regulated entity should consider stress testing such scoring systems against a range of scenarios, in accordance with its internal risk tolerance.

Example – Numerical Risk Scoring System

53. Below is an example of a customer risk assessment methodology which considers all four of the required risk factors equally.

54. Please note that each of the figures provided in this section are purely for illustration purposes only and are not intended to be used obligatorily by a regulated entity. A regulated entity should determine what risk weighting it considers appropriate, in line with its assessment of its risk profile.

Risk Element	Risk Score	Risk Weighting
Customer risk		25%
Product risk		25%
Interface risk		25%
Country risk		25%

55. As noted above, the risk weightings for each of the four elements should be considered and adjusted, according to the regulated entity's own business risk assessment. For example, if a regulated entity considers that its exposure to interface risk is low and does not typically vary between customers, this element could be assigned a lower risk weighting, and the risk weighting be redistributed to a risk element considered of higher importance. This is outlined in the example below.

Risk Element	Risk Score	Risk Weighting
Customer risk		30%
Product risk		30%
Interface risk		10%
Country risk		30%

56. Other risk elements may be considered in line with the regulated entity's own business risk assessment. If a regulated entity has determined that a particular risk element is material, it should be considered within the client risk assessment methodology.

57. The customer should then be risk scored against the risk posed by each particular element. A regulated entity should develop clear guidelines and factors for the scoring of each risk, in line with its assessment of its client base and risk tolerance. In the example provided below, a scale of 1-5 is used with 1 being the lowest risk factors and 5 being the highest risk factors. The weighting is then cumulatively tallied to create an average overall risk score.

Risk Element	Risk Score	Risk Weighting
Customer risk	4	25%
Product risk	5	25%
Interface risk	5	25%
Country risk	3	25%
	Overall risk score	**4.25 (HIGH**

58. The overall numerical risk score provided above will then determine the level of due diligence and monitoring required to be applied to that customer. Regardless of the overall score arrived at, the presence of risk in a particular area may lead to the determination that additional

mitigating measures are required. For example, in the case of increased interface risk, this may lead to a regulated entity taking additional measures to verify the identity of the customer.

59. It should be noted that the presence of mandatory high risk factors (such as PEP status or establishment in a high risk jurisdiction) should automatically lead to the treatment of the customer as high risk. This is regardless of the overall numerical risk score achieved. This has been set out in the example below, where the identification of such factors automatically leads to an overall risk score of 100.

Risk Element	Risk Score	Risk Weighting
Customer risk	PEP	25%
Product risk	1	25%
Interface risk	1	25%
Country risk	1	25%
	Overall risk score	**100 (HIGH)**

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