GIBRALTAR FINANCIAL SERVICES COMMISSION

3. Business Risk Assessment

GFSC AML/CFT/CPF Guidance Notes

Table of Contents

3.1 Purpose of the Business Risk Assessment

AML/CFT/CPF Requirements

R6 A regulated entity must take appropriate steps to identify and assess the risks of money laundering, terrorist financing and proliferation financing posed by its operations. This assessment must take into account all relevant risk factors pertaining to the regulated entity's operations, including but not limited to:

a) The nature of the products and services offered;
b) The nature of the client base;
c) The jurisdictions where services are provided or that are involved in the provision of those services; and
d) The channels through which its products and services are delivered.

R7 The business risk assessment should be documented, proportionate to the size and nature of the regulated entity's business, and kept current on an ongoing basis.

Guidance

1. In accordance with the Act, a regulated entity must take appropriate steps to identify the ML, TF & PF risks faced by its business operations[1]. The business risk assessment should form the basis for the regulated entity's policies, procedures, methodologies, controls and standards relating to AML/CFT/CPF. This should form part of the regulated entity's wider risk management framework.

2. Fully understanding the inherent risks associated with a regulated entity's operations allows that entity to determine what its risk appetite is (i.e. what subsequent business relationships it is willing to establish or not). For those business relationships that fall within its risk appetite, the regulated entity must determine what controls it will have in place to mitigate the level of risk posed by that relationship. 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 relationship/client. For more information on these requirements, please refer to the Client Risk Assessment section within these Guidance Notes.

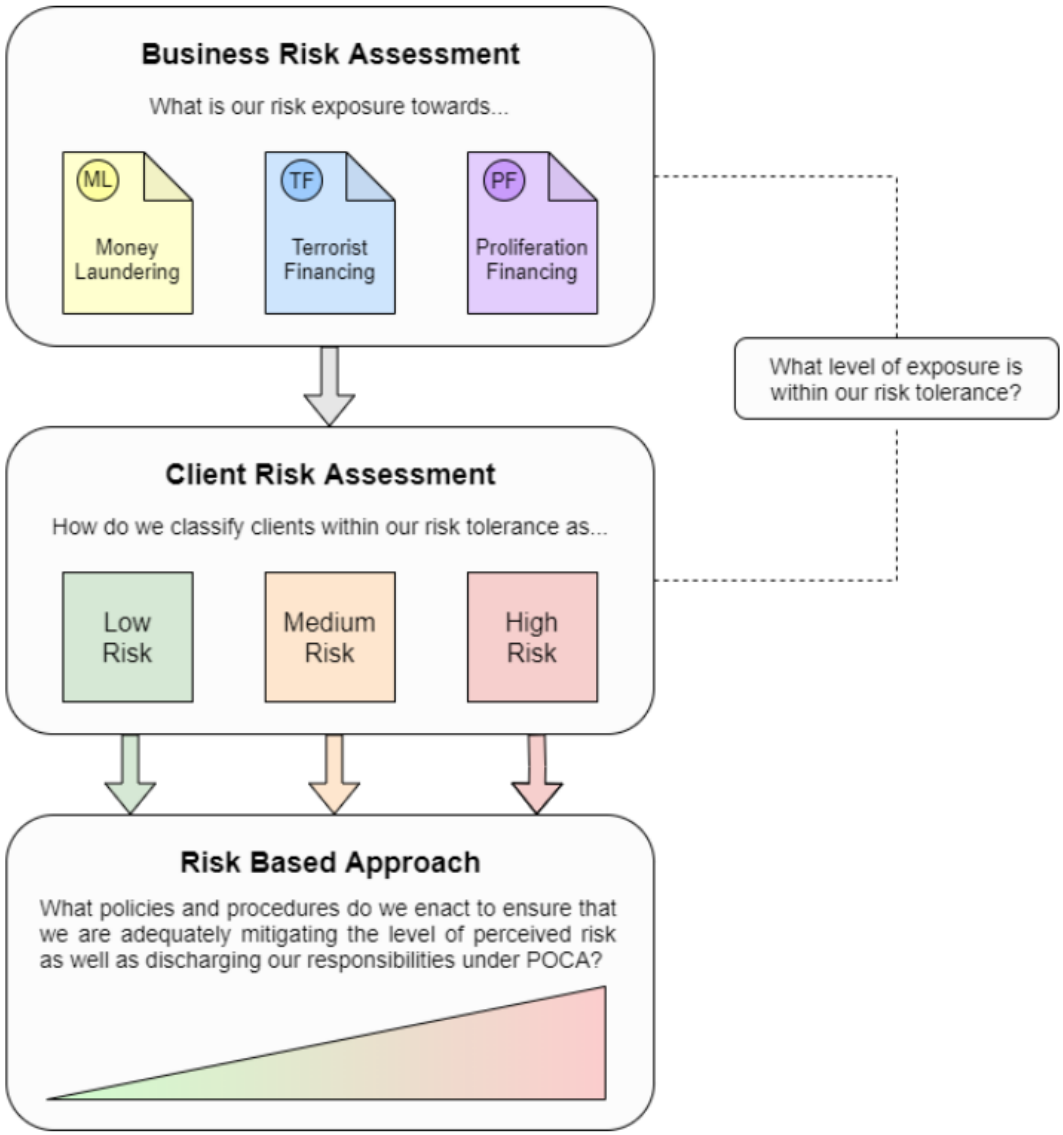
3. The principle of proportionality ensures that each regulated entity is able to determine bespoke systems of control that are suitable to the size and nature of its business, while adequately combating the risk of ML/TF/PF and discharging its obligations under the Act. It is therefore the responsibility of each regulated entity to determine the method in which it will identify, assess and mitigate the ML/TF/PF risks faced by its business operations.

4. A regulated entity must also be able to demonstrate that its assessment of ML/TF/PF risks is documented and accessible. This is both to ensure that the information is available to the relevant competent authorities (such as the GFSC) when requested, as well as to warrant that relevant members of staff are fully aware of the ML/TF/PF risks faced by the business.

5. Figure 1 visually demonstrates the relationship between the business risk assessment, client risk assessments and the implementation of a risk-based approach.

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

Figure 1 – Business risk assessments, client risk assessments & the risk-based approach.



3.2 The National Risk Assessment ("NRA")

AML/CFT/CPF Requirements

R8 The business risk assessment carried out by a regulated entity must take into account the threats, vulnerabilities and risks identified within the most recent version of HM Government of Gibraltar National Risk Assessment.

Guidance

6. In April 2016, HM Government of Gibraltar published the first NRA, setting out its assessment of the money laundering and terrorist financing threats, vulnerabilities and risks faced by the jurisdiction. The identification and assessment of these factors within the NRA is an iterative process. When procuring or updating a business risk assessment, a regulated entity must ensure that it makes use of the most recent iteration of the NRA.

7. The FATF defines the NRA as "an analysis of the threats, vulnerabilities and risks in a money laundering and terrorist financing context". The analysis of the Gibraltar NRA extends to the local threats, vulnerabilities and risks identified in association with proliferation financing.

8. In practice, the assessment is led by Gibraltar's National Coordinator for AML/CFT/CPF. In developing each iteration of the NRA, both public and private sector input is sought to ensure that all relevant risks are thoroughly and accurately identified, assessed and documented.

9. The purpose of the NRA is to provide a realistic analysis of the strengths and weaknesses in the fields of ML, TF & PF, and to identify existing and future risks and map them effectively. In order for a regulated entity to form an accurate assessment of the risks associated with its operations, this assessment must take into account the factors identified within the NRA for its particular sector and business activities.

3.3 Conducting the Business Risk Assessment

10. As detailed above, it is the responsibility of each regulated entity to determine the method by which it conducts its business risk assessment. The execution of the business risk assessment, however, should in some form encompass the following basic steps:
    a. Identification of the inherent ML, TF & PF related risks associated with the business model;
    b. Assessment/scoring of each of the identified risks;
    c. Identification and application of risk-based controls;
    d. Assessment of the level of residual risk, considering the implementation of the controls; and
    e. Identification/application of any additional controls outside of the business' risk tolerance.

11. The risk assessment process should be continuous, in that each regulated entity must periodically review the assessment to ensure that it still adequately encompasses all risks. As an example, deviation in business model or client base may mean that a business' risk exposures may change. Prior to the launch of any new products or services, a regulated entity must ensure that it has assessed the ML, TF & PF risks attributed to those products or services. Advancements in technologies, trends and vulnerabilities in the exploitation of financial businesses for the purposes of facilitating financial crime may also pose additional risks that may not have been originally considered. It is therefore imperative that the business remains continuously informed of both its regulatory obligations, and the progression of international standards.

12. A regulated entity is able to seek professional assistance in conducting the risk assessment should it consider that appropriate. The obligations, responsibilities and liabilities under the Act, however, will remain with the regulated entity. It is therefore the responsibility of the regulated entity to ensure that the assessment adequately addresses the risk exposure of its business operations.

3.3.1 Identification of ML, TF & PF Risks

13. A regulated entity's inherent exposure to risks relating to ML, TF & PF should be assessed by considering the following factors:
    a) The nature of the products and services offered;
    b) The nature of the client base;

c) The jurisdictions where services are provided or that are involved in the provision of those services; and
d) The channels through which its products and services are delivered.

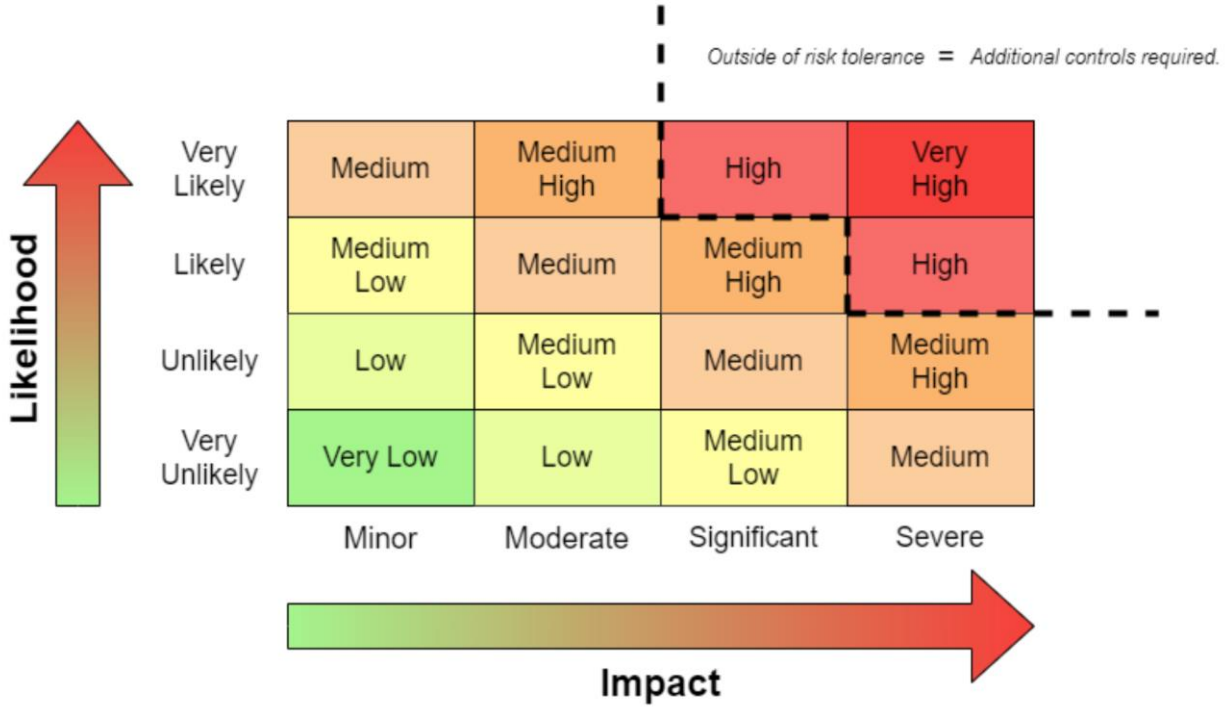
14. The nature of the risks associated with ML, TF & PF are often distinct and may vary in line with consideration of each of the above factors. A particular set of activities, for example, may exhibit a greater level of inherent vulnerability to one form of financial crime, while being less likely to be exploited for another. The individual conducting the risk assessment must therefore have a robust understanding of the characteristics which may impact the assessment of ML, TF & PF.

15. A regulated entity may employ varying methodologies when scoring the inherent/residual risks associated with its business operations. The scoring process allows a regulated entity to determine which risks may be outside of its tolerance levels and may require the implementation of additional mitigating controls.

Case Study – Example Risk Scoring Matrix

16. Figure 2 below shows an example of a risk scoring matrix which relies on an assessment of the likelihood of a risk materializing, as well as the impact of that risk taking place. Please note that a regulated entity is required to adequately document whichever scoring parameters are used for its assessment.

Figure 2 – Example risk scoring matrix



Guidance

3.3.2 Application of Risk Mitigation Controls

17. Once all inherent ML, TF and PF-related risks associated with the regulated entity's business operations have been identified and assessed, the entity must then determine what controls must be put in place in order to mitigate that risk and satisfy its regulatory and legislative

requirements. This should be carried out on a continuous basis in order to assess both existing and novel risks.

18. When determining risk appetite, a regulated entity should form an understanding of what level of risk is considered to be outside of its risk tolerance. Risks that arise outside of this should therefore trigger the need to establish additional controls. The persistence of risks outside a business' risk tolerance may also be indicative that the regulated entity should re-assess its risk appetite criteria.

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