Guidance on the Risk-Based Approach

TABLE OF CONTENTS

Version control:

Guidance on the Risk-Based Approach
V5.0
March 2020

GLOSSARY OF TERMS

ABC	Anti-Bribery and Corruption
AML/CFT	Anti-Money Laundering/Combating Terrorist Financing
AML/CFT Law	State of Qatar Law No. [20] of 2019 on Combating Money Laundering and Terrorism Financing
BO	Beneficial Owner
CDD	Customer Due Diligence
DNFBP	Designated Non-Financial Business and Profession
FATF	Financial Action Task Force
FI	Financial Institution
FIRM	Financial Institution and Designated Non-Financial Business and Profession
FSRB	FATF-Style Regional Body
HROMJ	High Risk or Other Monitored Jurisdiction
KYC	Know Your Customer
ML	Money Laundering
NCTC	National Counter Terrorism Committee (Qatar)
PEP	Politically Exposed Person
QFC	Qatar Financial Centre
TF	Terrorist Financing
UBO	Ultimate Beneficial Owner

1. PURPOSE

The purpose of this guidance is to:

- indicate good industry practice in AML/CFT procedures through a proportionate, risk-based approach; and
- assist firms to design and implement the systems and controls necessary to apply a risk-based approach that effectively mitigates the risks of the firm being used in connection with money laundering and the financing of terrorism.

The guidance does not address every possible scenario and is not to be interpreted as legal advice. Firms must develop AML/CFT policies, procedures, systems and controls that are appropriate for the nature, scale and complexity of their respective businesses.

The guidance does not replace AML/CFT legislation[1] applicable in the State of Qatar or the Qatar Financial Centre. Firms remain responsible for compliance with legislation that is relevant to their operations.

This guidance is intended to assist Firms to develop a Risk-Based Approach (RBA) to managing their Money Laundering (ML)/Terrorist Financing (TF) risks. It consists of the following:

- general information about risk management frameworks that Firms may wish to consider in developing and implementing a risk-based approach to identify, mitigate, and manage ML/TF risks;
- guidance to assist Firms in implementing a risk-based approach (RBA), including guidance on developing a Threat Assessment Methodology, conducting a Business Risk Assessment, undertaking risk profiling and scoring business relationships, and ensuring appropriate risk mitigation; and
- guidance and information to assist Firms on dealing with higher risk countries.

[1] The term "legislation" is used throughout in its broadest sense, to cover all elements of the legislative framework, including laws, regulations, rules, etc.

2. RISK MANAGEMENT FRAMEWORK

The risk management framework discussed in this guidance aims to assist Firms to develop and implement their AML/CFT programme, and to ensure that a RBA is adopted to identify, mitigate, and manage ML and TF risks.

Firms are required to develop a programme against ML and TF. Firms are best placed to assess ML/TF risk(s) they may face in conducting business, having regard to the size, nature, and complexity of their business. Firms have the flexibility to construct their risk management frameworks for the purpose of developing risk-based systems and controls (proportionate to the ML/TF risk(s) faced) and mitigation strategies in the manner most appropriate to their business structure and the products and/or services they provide to customers.

Regulators expect Firms to develop and maintain logical, comprehensive, and systematic methods to address each of the components referred to in this guidance; and that such methods and the approach to ML/TF risk are implemented within their organisations.

Firms are expected to demonstrate that their risk-based policies, procedures, systems, and controls are suitable to their particular businesses (having regard to their size, nature, and complexity) and are consistent with prudent and good practice. A well-reasoned and effective RBA relevant to a firm's business and circumstances should assist the Firm to manage ML/TF risks it may face.

Firms must periodically review and evaluate their risk management framework to ensure that it is effective, and to identify improvement opportunities that may arise.

The following are relevant extracts from Qatar's 2019 AML/CFT Law:

Article (6)

"Financial institutions and DNFBPs shall identify, consider, understand, assess, document, monitor and update, on a regular basis, their ML/TF risks; and shall submit relevant reports to the Supervisory Authorities, upon request.

Financial institutions and DNFBPs shall consider the risks that may arise from the development of new products, new business practices or new techniques, prior to the use of such products, practices and techniques.

Financial Institutions and DNFBPs shall also take into consideration the risks identified at the national level and any other underlying factors.

Article (7)

"Financial institutions and DNFBPs shall adopt a risk-based approach, by developing risk-based internal policies, procedures and controls. Financial institutions and DNFBPs shall effectively implement these policies, procedures and controls to manage the risks identified; including those identified in the National Risk Assessment, and shall mitigate

these risks in line with the nature and size of their businesses. Financial institutions and DNFBPs shall, where appropriate, review, update and enhance these policies, procedures and controls.

They shall also apply these internal policies, procedures and controls on all their branches and majority owned subsidiaries."

FATF Recommendation 1- Assessing risks and applying a risk-based approach

"Countries should identify, assess, and understand the money laundering and terrorist financing risks for the country, and should take action, including designating an authority or mechanism to coordinate actions to assess risks, and apply resources, aimed at ensuring the risks are mitigated effectively. Based on that assessment, countries should apply a risk-based approach (RBA) to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified. This approach should be an essential foundation to efficient allocation of resources across the anti-money laundering and countering the financing of terrorism (AML/CFT) regime and the implementation of risk-based measures throughout the FATF Recommendations. Where countries identify higher risks, they should ensure that their AML/CFT regime adequately addresses such risks. Where countries identify lower risks, they may decide to allow simplified measures for some of the FATF Recommendations under certain conditions.

Countries should require financial institutions and designated non-financial businesses and professions (DNFBPs) to identify, assess and take effective action to mitigate their money laundering and terrorist financing risks."

3. DEVELOPING THE AML/CFT PROGRAMME

Firms should have particular focus on the key requirements of the relevant legislation that constitute the building blocks for developing and implementing the programme. The senior management of a Firm must ensure that the Firm's policies, procedures, systems, and controls appropriately and adequately address the requirements of the legislation.

The type and extent of the measures adopted by the Firm as part of its programme must be appropriate in regard to the risk of ML/TF and the size, complexity, and nature of its business.

All Firms must retain relevant records for at least ten years. Firms must ensure that all the records can be retrieved without undue delay.

4. INDEPENDENT REVIEW AND TESTING

A Firm's programme against money laundering and terrorist financing must include "an independent review and testing of the Firm's compliance with its AML/CFT policies, procedures, systems and controls".

In the current context of risk assessments, Firms are required to ensure that an independent review and testing is conducted on their risk assessment policies, procedures, systems, and controls including the Business Risk Assessment, Threat Assessment Methodology and risk profiling of business relationships, to review whether they are appropriate for the nature, scale, and complexity of the Firm, and whether they remain fit for purpose.

5. GUIDANCE ON THE RISK-BASED APPROACH

In line with FATF Recommendation 1 (and other relevant Recommendations and Interpretative Notes) and the relevant legislation, Firms should adopt a RBA by developing risk-based internal policies, procedures, and controls.

The RBA is a management tool for developing and managing a Firm's systems and controls. Firms should involve senior management in the managing of their risks and using their knowledge of the Firm to develop systems that uniquely address the specific risks that they face. The RBA allows Firms to allocate focus resources, or apply additional resources, to areas of high risk.

There will always be a requirement for Firms to monitor their customers' activities, but the specifics of how this is done can vary greatly depending on the nature of the risks they face and the type of products they sell. For example, a large bank with many customers will likely need to develop or purchase transaction monitoring software, whereas a smaller organisation may be able to monitor its customers using a less sophisticated solution.

The terms risk, threat, vulnerability, and consequence are often used by FATF when describing how jurisdictions should implement AML/CFT standards. These terms mean:

- **Risk** can be seen as a function of three factors: threat, vulnerability, and consequence. An ML/TF risk assessment is a product or process based on a methodology, agreed by those parties involved, that attempts to identify, analyse, and understand ML/TF risks and serves as a first step in addressing them. A risk assessment involves making judgments about threats, vulnerabilities, and consequences, which are discussed below.

  The size and seriousness of a given risk is a function of the likelihood of ML or TF activity occurring, and the consequences of or harm caused by that occurrence. Thus, the co-existence of threats and vulnerabilities that could result in significant consequences or harms would be considered "high risk".

- **A threat** is a person or group of people, object, or activity with the potential to cause harm to, for example, the state, society, the economy, etc. In the ML/TF context this includes criminals, terrorist groups and their facilitators, their funds, as well as past, present, and future ML or TF activities. Threat is described above as one of the factors related to risk, and typically it serves as an essential starting point in developing an understanding of ML/TF risk.

- **Vulnerabilities** are the intrinsic properties in a system or structure (including weaknesses in systems, controls, or measures) which make it open to abuse or exploitation by criminal elements for ML, TF, or both. The existence of vulnerabilities in a system makes that system attractive for money launderers and terrorist financers to use.

- **Consequence** refers to the impact or harm that ML or TF may cause, and includes the effect of the underlying criminal and terrorist activity on financial systems and institutions, as well as on the economy and society more generally. The consequences of ML or TF may be short- or long-term in nature, and also relate to populations, specific communities, the business environment, or national or international interests, as well as the reputation and attractiveness of a country's financial sector.

A. The Business Risk Assessment: frequently asked questions

A Firm must be able to demonstrate that it has considered its exposure to ML/TF risks. The Business Risk Assessment must be documented and receive senior management's approval.

It is important for Firms to establish and document their risk appetite, which defines the type, level, and extent of risks a Firm is willing to expose itself to, for the furtherance of its business activities. Senior management's involvement and sign off is an integral part of the process, as this could have an impact on the profitability and/or regulatory obligations of a Firm.

Firms must take care to include only risk factors which relate to ML/TF, and not wider risks such as financial soundness, credit, market, liquidity, complaints, etc.

1. What is the purpose of a risk assessment?

The key purpose of an ML/TF risk assessment is to drive improvements in risk management through identifying the general and specific ML/TF risks a Firm is facing, determining how these risks are mitigated by its AML/CFT programme controls, and establishing the residual risk that remains.

The results of a risk assessment can be used for a variety of reasons, including:

- Identify gaps or opportunities for improvement in AML/CFT policies, procedures, and processes;
- Make informed decisions about risk appetite and implementation of control efforts, allocation of resources, and technology spend;
- Assist management in understanding how the structure of a business unit or business line's AML/CFT compliance programme aligns with its risk profile;
- Develop risk mitigation strategies. including applicable internal controls, and therefore lower a business unit or business line's residual risk exposure;
- Ensure senior management are made aware of key risks, control gaps, and remediation efforts;
- Assist senior management with strategic decisions in relation to commercial exits and disposals;
- Ensure regulators are made aware of key risks, control gaps and remediation efforts across the Firm; and
- Assist management in ensuring that resources and priorities are aligned with its risks.

2. How often should a risk assessment take place?

The frequency of the risk assessment will depend upon a number of factors, including the methodology employed, the validation process, audit reviews and associated

action plans, the results of the previous risk assessment, etc. Regulators expect that a risk assessment be reviewed at a minimum on an annual basis, or more frequently due to internal trigger events such as changes in its customers, business, products, services, technologies, or the jurisdictions it deals with, or due to external triggers such as changes in the market, implementation of or changes to sanctions programmes, or changes in applicable legislation.

Regardless of the frequency of risk assessments, Firms are usually required to report annually (such as the Annual MLRO Report) on the status and effectiveness of the ML/TF risk environment. Additionally, ad hoc risk assessments may be performed, focusing on higher risk areas and the specific controls that have been implemented to address the given risk. The results from these ad hoc risk assessments can then be incorporated into the next regular ML/TF risk assessment.

3. How should a risk assessment be organised?

Whichever approach is chosen, Firms should ensure that their approach is logical, clearly documented, and approved by senior management. The methodology for the risk assessment must be clearly articulated, especially with regard to the factors being assessed and the criteria used to score them, the requisite weightings used in the scoring methodologies, any scoring overrides applied, including the rationale for them and any business line/business unit specific parameters, amongst others. While arbitrary scoring overrides should not be the norm and may potentially reflect a flaw in the methodology, there may be instances where a manual override is necessary, especially in the first few times a risk assessment is conducted and until such a time as the methodology employed stabilises.

The decision as to who owns and manages the risk assessment may be impacted by how the risk assessment is conducted, i.e. whether by business lines, country, region or enterprise-wide, and the decision will be influenced by the structure, global footprint, and complexity of a Firm. For enterprise-wide risk assessments, a number of risk assessments may be aggregated to a single level to become enterprise-wide, although tactical actions may be owned at a business line level rather than at a Firm-wide/Group level. Strategic actions are likely to be owned and driven at a Group or regional level. The owners of actions may differ according to the size and complexity of the Firm, but should be those individuals who are accountable for ensuring the action can be completed.

4. What should be the scope of the risk assessment?

The scope of a risk assessment should be clearly articulated, i.e. whether it is a risk assessment that is independent from the business and conducted by the Compliance function, or whether it is an integrated risk assessment, capturing issues identified by both business and Compliance. Whichever approach is chosen, the risk assessment should focus on AML/CFT risk. A Firm's senior management and MLRO are responsible and accountable for understanding the extent of those risks, and the MLRO should understand the effectiveness and deficiencies of the Firm's corresponding mitigating

controls, irrespective of whether the MLRO owns the management and maintenance of those controls.

5. Whose responsibility is it to undertake a risk assessment?

Senior management of a Firm are the overall owners of the risk environment. They may delegate the assessment of risk to appropriately qualified, expert staff such as the Legal/Financial Crime Compliance/AML Unit/MLRO, which may have primary responsibility for the initiation and delivery aspects of the ML/TF risk assessment. This would include tasks such as methodology development, maintenance, periodic refresh process/activity initiation, and record keeping of completed assessments. Business line heads, as well as other departments, such as Information Technology, Operational Risk, and Payments, for example, may also be required to contribute. It is to be noted that, while the Firm's senior management may delegate the risk assessment process, the ownership of the risks remains firmly with the business, who may also be responsible for carrying out any actions resulting from the gaps or deficiencies identified by the risk assessment exercise.

The purpose of the risk assessment and the contribution required from each party should be clearly outlined, with Firms considering whether to include specific responsibility for contribution to, and the execution of, the risk assessment as part of the annual performance objective setting process for relevant staff. Firms should also ensure that timely and appropriate training/guidance is provided to staff involved in the completion of the risk assessment to ensure that a consistent approach is taken, e.g. in relation to the meaning of specific terminology.

The chosen risk assessment framework should be fully endorsed by a Firm's senior management, and used as one of the tools through which a culture of compliance can be driven. Senior management/the MLRO should ensure there are adequate resources allocated to managing the risk assessment process and its outcomes.

6. What are the factors to consider?

In conducting a Business Risk Assessment, Firms need to consider the following (see **Figure 1** for an example of a threat Matrix):

- the threats, risks, and vulnerabilities identified in the National Risk Assessment, and any Sectoral Risk Assessment, published by Competent Authorities;
- the involvement of senior management in deciding the risks posed by ML/TF;
- the organisational factors that may increase the level of exposure to the risk of ML/TF;
- the nature, scale, and complexity of its business, the diversity of its operations (including geographical diversity), the volume and size of its transactions, and the degree of risk associated with each geographic and functional area of its operations;
- who its customers are, and the nature of their economic activity;

- whether any additional risks are posed by the jurisdictions with which its customers (including intermediaries and introducers) are connected. (Factors such as high levels of organised crime, increased vulnerabilities to bribery and corruption, and inadequate frameworks to prevent and detect ML/TF, will impact the risk posed by relationships connected with such jurisdictions);
- the characteristics of the products and services that it offers and assessing associated vulnerabilities posed by each product and service, including delivery channels; and
- how it establishes and delivers products and services to its customers. (For example, risks are likely to be greater where relationships may be established remotely (non-face to face), or may be controlled remotely by the customer (straight-through processing of transactions).

7. What should a Firm do with the issues highlighted during a risk assessment?

The completion of a risk assessment may indicate gaps or deficiencies in the control environment. These should result in actions that are prioritised appropriately and tracked centrally. Ownership of these actions may be allocated to different parts of the business, but the MLRO should have oversight of the completion of these actions.

Actions raised may have a significant impact on the residual risk rating once they are completed, and therefore must receive utmost attention and support from senior management and other relevant stakeholders. It is recommended that, wherever possible, the actions raised be remediated before the next risk assessment is carried out, in order to assess whether or not the residual risk position has improved. Senior management must justify the non-completion of an action beyond a reasonable timescale. Ongoing non-completion of an action should lead to further escalation.

The issues highlighted during a risk assessment may impact annual planning, monitoring and testing, and management information data across a Firm. As such, there should be a sufficiently robust quality assurance process to check whether proposed actions appropriately address the issues raised, including senior management's tracking of progress on action closures.

8. What next after a risk assessment?

Subsequent to a risk assessment, the following would generally be the next steps:

- communicate the results to individual business divisions, senior management, and other stakeholders;
- compare current and previous risk assessments to determine if the risk rating has increased, decreased, or remained constant;
- Senior management/the Board need to discuss and determine if the risk rating is within the risk appetite (and risk tolerance) of the Firm, keeping in

mind its strategic goals;

- consider and mitigate any new inherent risks identified;
- fix the gaps identified in the control environment; and
- consider an independent review and testing of the AML/CFT programme.

Refer to **Appendix 1** for an illustrative example of a Business Risk Assessment.

B. **The Business Risk Assessment: a three-step process**

Step 1. Identifying the Inherent Risks.

Step 2. Assessing the Control Environment - mitigating, managing, control, monitoring, and periodic reviews.

Step 3. Arriving at the Residual Risk – the final AML/CFT risk of the Firm.

Step 1. Identifying the Inherent Risks.

Inherent Risks represent the exposure to ML/TF and other risks such as sanctions or bribery and corruption, in the absence of any control environment being applied. A Firm's approach to categorising risks should be clearly documented.

- Customers
- Products and services
- Interface/delivery channel
- Jurisdictions
- Other qualitative risk factors specific to the nature, scale, and complexity of the Firm (reputation, regulatory, criminal, etc.)

The categories of risk faced by an organisation can be very broad. These broad risk categories are then sub-divided into inherent risk factors that are derived from regulatory guidance or expectations, such as the categories outlined below, as well as leading industry practices, and include a mix of both qualitative and quantitative criteria. Risk factors are the underlying causes or circumstances where a Firm may be used for purposes connected to ML or TF.

Managing the risk factors inadequately could lead to the Firm being exploited for ML or TF, which in turn could lead to reputational harm, regulatory penalties, legal sanctions, and consequent financial costs. Due to the nature of the particular business unit or business line's products and services and customer base, a RBA is used to determine inherent risks. Each risk factor is usually assigned a score and weighting which reflects the level of risk associated with that risk factor, and the prevalence of that risk compared to other risk factors.

Customers

For the purposes of assessing the inherent ML/TF risk of a business division, unit, or business line, the customer base and business relationships should be assessed. A number of customer types, industries, activities, and professions and businesses, alongside other factors, such as the length of a customer relationship, can increase or decrease ML/TF and other risks. The following categories can be used to stratify the customer base and to identify aspects of customer risk: customer type, ownership, industry, activity, profession and/or business. Some, or all, of these

categories may be relevant depending upon the particular division, unit, or business line under review.

Each customer type is assigned a risk score, depending upon the expected scale of ML/TF risk each type carries. For the business division, unit, or business line in question, the number of customers that fall within each customer type should then be determined/estimated. This data can be utilised to determine what percentage of each business division, unit, or business line customer types are rated according to the Firm's risk classification model, e.g. low, moderate, high, very high risk, in order to determine the overall inherent customer risk.

Products and services

One of the other major risk components can be found when considering Products and services risks, where a Firm will seek to identify its portfolio of main products/account types and assign an inherent score (e.g. low, moderate, etc.) to each, based on its general inherent characteristics and the degree of ML/TF and other risks present. For the business division, unit, or business line in question, the number of products/account types offered by the business, and (if available), associated account balances or, where relevant, turnover, should then be determined/estimated. This data can be utilised to determine what percentage of each business division, unit, or business line products/account types are rated according to the risk classification e.g. low, moderate, etc., in order to determine the overall inherent product risk.

Interface/delivery channel

Some delivery channels/servicing methods can increase ML/TF and other risks because they increase the risk that the division, unit, or business line does not truly know or understand the identity and activities of the customer. Consequently, it should be assessed whether, and to what extent, the method of account origination or account servicing, such as non-face-to-face account opening or the involvement of third parties, including intermediaries, could increase the inherent ML/TF risk. It should be noted that these accounts may not always lead to an increase in the inherent ML/TF risks, e.g. where the customer is known to the Firm but undertakes business activities non-face-to-face. Non-regulated customers, or those that are not well known to a Firm, are much more likely to present a higher inherent risk of ML/TF and other risks.

For this risk category, the business division, unit, or business line will then determine/estimate the percentage of accounts or customers that are rated according to the risk classification e.g. low, moderate, etc., in order to determine the overall inherent channels risk.

Geography/country

Identifying geographic locations that may pose a higher risk is a core component of any inherent risk assessment, and the business division, unit, or business line must

understand and evaluate the specific risks associated with doing business in, opening and servicing accounts, offering products and services and/or facilitating transactions relating to certain geographic locations.

The geography/country risk may also be analysed with respect to the location of the business division, unit, or business line, and may also include its subsidiaries, affiliates, and offices, both internationally and domestically. The aim is to identify the geographic footprint of a Firm. For customers, the aim is to identify the number of its customers within each country. The Firm will need to decide whether this number should be based on all or some of the following: domicile, incorporation, and nationality. In order to map geographies/countries into different risk ratings, a Firm's own country risk model, or equivalent (appropriately reviewed) third party vendor product, may be used.

Geography/country risk may also be considered together with some of the other risk factors in other risk categories, such as customers holding dual nationality involving a high risk country. The percentage of a business division, unit, or business line's transactions with a high risk country may provide an indication of the inherent risk from a geography/country perspective.

Geography/country risk will be important in any sanctions risk assessment, not only with respect to sanctioned countries themselves, but also those that may have well known/important links or other significant connections to sanctioned countries. These could include countries bordering, or in close proximity to, sanctioned countries, or those countries which present potential opportunities for the diversion of funds with the intent to violate or circumvent sanctions regulations.

Additionally, geography/country risk will also be applicable in any assessment of ABC risk. Certain jurisdictions carry increased levels of bribery and corruption risk, usually to do with how those in power are able to abuse their positions for their own financial gain. Where such jurisdictions are present in a Firm, the bribery and corruption risks need to be appropriately reflected.

For more details, refer to **GUIDANCE ON HIGHER RISK COUNTRIES.**

Qualitative risk factors

Additional risk factors can have an impact on operational risks, and contribute to an increasing or decreasing likelihood of breakdowns in key AML/CFT controls. Qualitative risk factors directly or indirectly affect inherent risk factors. For example, significant strategy and operational changes, such as the introduction of a major new product, or service, a merger or an acquisition, opening in a new location or closing an entity, may affect the inherent risk.

These changes will require a review of existing internal controls and, depending on the circumstances, possibly the creation of new controls. Given that these controls may take some time to become effective, the division, unit, or business line will

need to assess whether the inherent risk may have temporarily increased. The main "Other Qualitative Risk Factors" might include:

- customer base stability;
- integration of IT systems;
- expected account/customer growth;
- expected revenue growth;
- employee turnover;
- recent AML Unit employee turnover;
- reliance on third party providers;
- recent/planned introductions of new products and/or services;
- recent/planned acquisitions;
- recent projects and initiatives related to AML Compliance matters (e.g. remediation, elimination of backlogs, off-shoring);
- recent relevant enforcement actions;
- Sectoral Risk Assessments;
- National Risk Assessments; and
- findings from regulatory assessments.

Step 2. Assessing the control environment

Once the inherent risks have been identified and assessed, internal controls must be evaluated to determine how effectively they offset the overall risks. Controls are programmes, policies, or activities put in place by the Firm to protect against the materialisation of an ML/TF risk, and to ensure that potential risks are promptly identified. Controls are also used to maintain compliance with regulations and rules governing a Firm's activities.

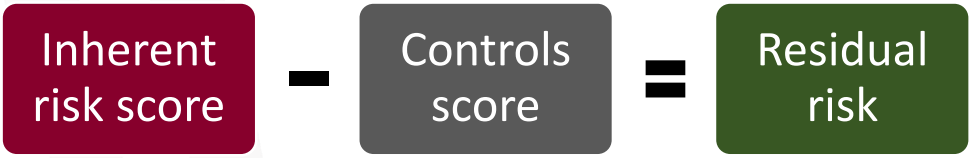
The control environment should factor in the following (not an exhaustive list):

- compliance culture;
- management oversight, responsibility, and accountability;
- roles and responsibilities of the MLRO and DMLRO;
- AML/CFT framework, Policies, Procedures, Systems, and Controls;
- Business Risk Assessment, Threat Assessment Methodology, and risk profiling of business relationships;
- KYC, CDD, and EDD;
- Suspicious Transaction Reporting;
- employee screening;
- the AML/CFT training programme;
- regulatory reporting/management reporting;
- documentary evidence of compliance, including record keeping and retention;
- monitoring and controls; and
- independent testing and sampling.

As with the illustrative inherent risk factors above, the response to each area under examination is assigned a score, which, when aggregated, reflects the relative strength of that control. Each area can then be assigned a weighting based on the importance that the institution places on that control. For example, it may be expected that CDD carries a larger weighting than record keeping and retention within the risk assessment.

Step 3. Arriving at the residual risk (final AML/CFT risk rating of the firm)

Once both the inherent risk and the effectiveness of the internal control environment have been considered, the residual risk can be determined. Residual risk is the risk that remains after controls are applied to the inherent risk. In effect, it is the score derived after deducting the control risk score from the inherent risk score.



The residual risk score then needs to be tied to a risk rating e.g. high, medium, or low, on a standard 3 tier rating scale. Firms can also implement a 5 tier rating scale of high, medium high, medium, medium low, and low. Firms should use a scale which best suits their business.

The residual risk is an important measurement that indicates whether the risks are being mitigated effectively.

Weighting and scoring

Factors such as business activities, products and services (including transactions), customer base, and geographic footprint, should be considered while calculating inherent risks. Each risk factor is usually assigned a score that reflects the associated level of risk. Each risk area may then be assigned a weight that reflects the level of importance in the overall risk calculation relative to other risk areas.

Similarly, each control may be assigned a weight that reflects the relative strength of that control. For example, if the focus of a business division within a Firm is correspondent banking, and a proportion of its customer base is in different international jurisdictions, geography will be of higher relevance (and therefore receive a higher weight) than, for example, a customer type for that business division. Similarly, certain controls have a more direct impact on the mitigation of ML/TF risk, such as front line controls where customer due diligence is weighted more heavily than controls around independent testing.

C. **Threat Assessment Methodology**

Firms are required to conduct their Business Risk Assessment based on a Threat Assessment Methodology, to enable the Firm to identify any changes in these risks, including risks posed by new products and services or new or developing technologies. A Firm may consider that frequent reassessments are appropriate in some cases (e.g. for a dynamic, growing business) and less frequent in other cases (e.g. an established business with stable products and services), and internal and external trigger events should always be considered when scheduling reassessments.

What is a Threat Assessment Methodology?

This is a methodology to identify and assess the threats a Firm faces in the environment it operates. The following important aspects are to be included in the preparation of a Threat Assessment Methodology:

- Consider and record the threats applicable to the Firm, its business model, and the environment it operates within. This enables the Firm and its stakeholders to understand what risks and actions are required to be taken by the Firm to mitigate these risks;
- The example of a threat matrix in Figure 1 is to be read in the context of the overall AML/CFT environment. Each Firm may have different views of these threats based on their own particular circumstances, which may increase depending on the degree of exposure that the particular Firm may have to the threat; and
- For the purposes of the threat matrix, the risk profile of threats will be measured in terms of their likelihood and impact. Predicate offences contained in the AML/CFT Law need to be taken into account in the Threat Assessment Methodology, as do common ML and TF typologies identified by international bodies and domestic Competent Authorities.

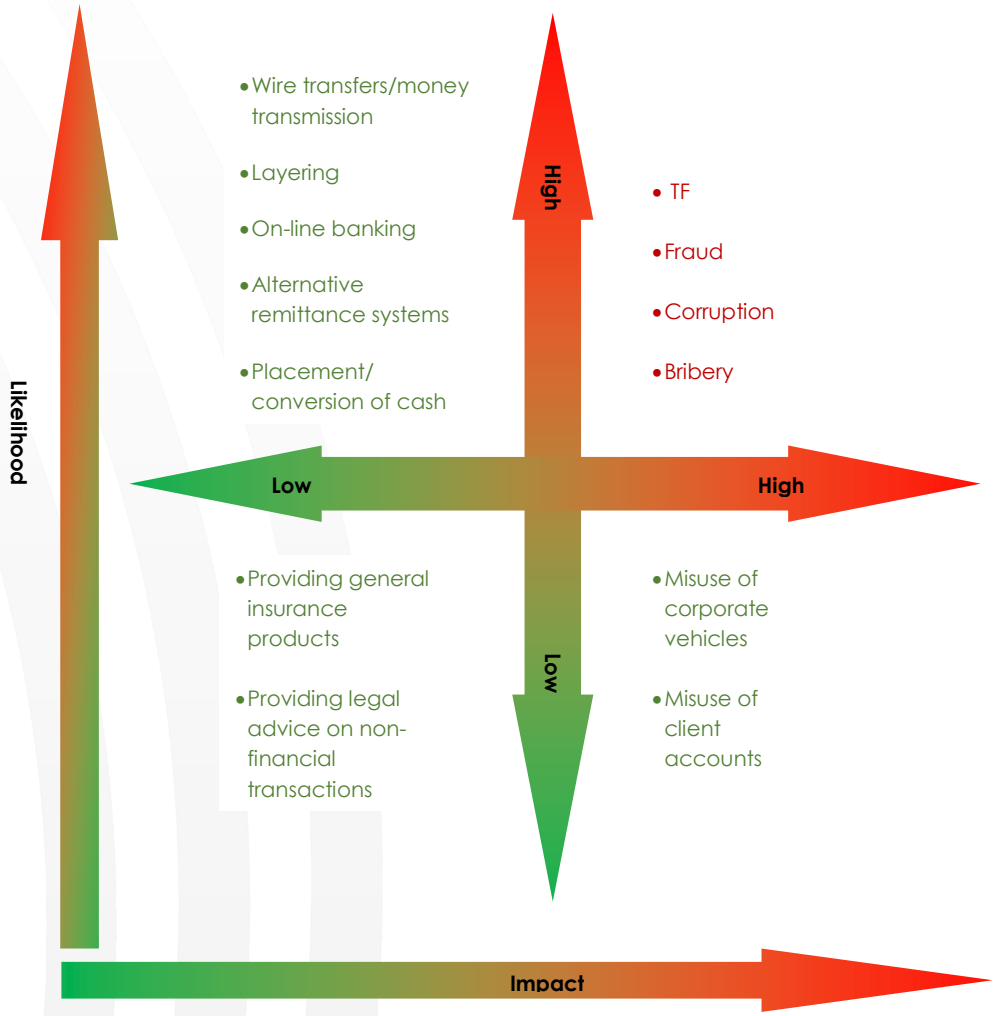


Figure 1 – Example of a threat matrix (the threats indicated are not exhaustive).

The matrix is divided into four quadrants: high impact and high likelihood threats, high impact and low likelihood threats, low impact and low likelihood threats, and low impact and high likelihood threats.

The further an item is placed to the right, the greater its impact will be. Similarly, the higher up on the matrix the threat appears, the greater the likelihood of its occurrence. The top right quadrant represents the highest risk category.

Refer to **Appendix 2** for the classification of threat factors.

D. **Risk Profiling of Business Relationships**

The purpose of risk profiling a business relationship is to provide the Firm with a clear understanding of the customer business relationship and the resulting level of customer due diligence (CDD) measures and ongoing monitoring required for the business relationship. Please refer to the guidance paper on CDD for further details.

At a minimum, Firms must consider all relevant risk factors (including the following 4 key risk factors), in developing the risk profile of a business relationship with a customer:

- customer risk
- product risk
- interface risk
- jurisdiction risk

Each risk factor is usually assigned a score that reflects the associated level of risk. Each risk factor may then be assigned a weight that reflects the level of importance in the overall risk calculation relative to other risk areas.

The total consideration of all of the risk factors combines to produce the risk profile of the business relationship, and that risk profile must be considered in deciding the extent of the CDD measures and ongoing monitoring to be conducted for the customer.

For certain types of products or services, it may be possible to prepare a risk profile on the basis of generic expected activity and transactions. For more complex products or services, however, more tailored activity profiles may be necessary.

In any event, a Firm must demonstrate that a risk profile of a business relationship contains sufficient information to enable it to identify:

- a pattern of expected business activity and transactions for each business relationship; and
- unusual or higher risk activity and transactions that may indicate ML/TF.

A comprehensive understanding of the risk presented by a business relationship may only become evident at a later stage following the establishment of the relationship. Dynamic use of new information will allow a Firm to demonstrate that it is regularly reassessing the risk profile, and that the CDD and ongoing monitoring approach reflects the customer risk.

Obtaining a risk profile

The four key risk factors (customer, product, interface, and jurisdiction), and any other risk elements, must be combined in order to provide the Firm with a risk profile for that business relationship.

As shown in **Appendix 3** on the scoring of risks, a Firm may choose, for example, to

allocate numerical values to the different constituents of each factor. In the example below, the factors have been given a maximum score of 10 each. By considering the characteristics, the total for each risk factor can be plotted on a simple chart.

Using pre-set criteria, the Firm can quickly assess the risk that a given business relationship poses to the Firm. Figure 2 below shows an example where the profile of the proposed business relationship is within the Firm's risk appetite. In this case, the Firm will need to perform standard due diligence.

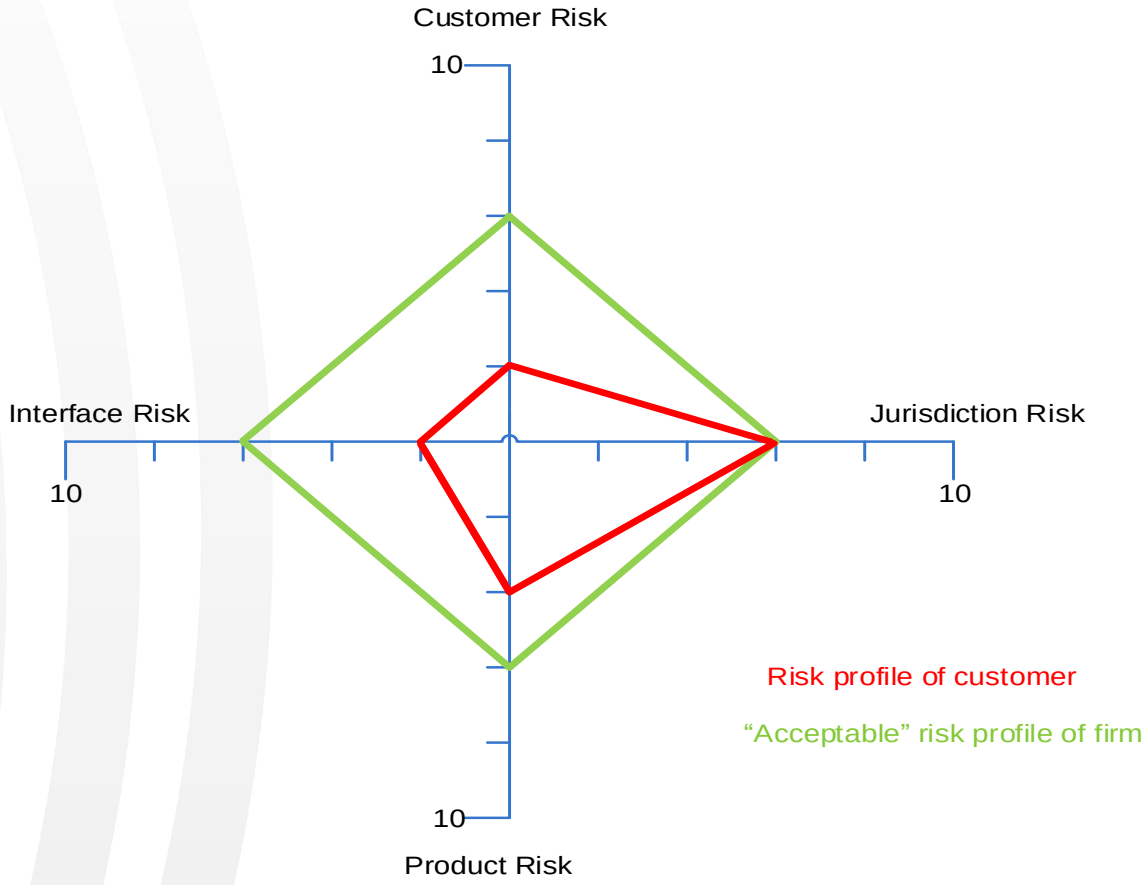


Figure 2: example of risk profiling where the customer profile fits within the firm's risk appetite

This method of illustrating risk is not obligatory, and Firms need to adopt a methodology that best suits them and their business model.

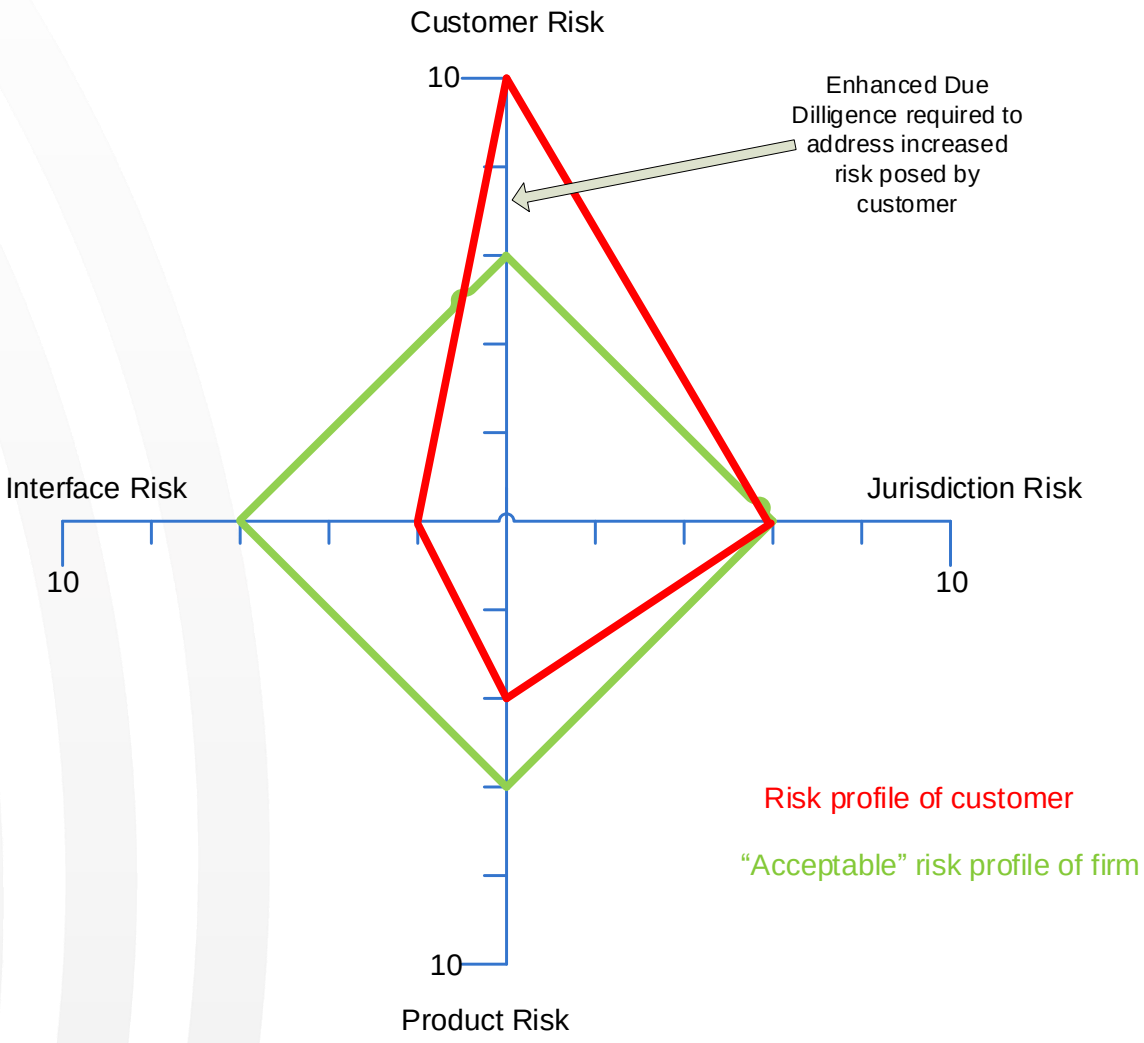


Figure 3: example of risk profiling where EDD is required

The Firm may be faced with a proposal to enter into a new business relationship where the customer's risk profile exceeds the Firm's own risk appetite. Two things can happen: the Firm can refuse to enter into the relationship, or, by taking further risk mitigation steps such as conducting additional due diligence checks on the customer, decide to accept it.

Refer to **Appendix 3** for risk scoring of business relationships.

6. GUIDANCE ON HIGHER RISK COUNTRIES

A. FATF Recommendation 19: higher-risk countries

"Financial institutions should be required to apply enhanced due diligence measures to business relationships and transactions with natural and legal persons, and financial institutions, from countries for which this is called for by the FATF. The type of enhanced due diligence measures applied should be effective and proportionate to the risks.

Countries should be able to apply appropriate countermeasures when called upon to do so by the FATF. Countries should also be able to apply countermeasures independently of any call by the FATF to do so. Such countermeasures should be effective and proportionate to the risks."

There is no universally agreed definition of a high-risk country, but when undertaking a country assessment, the following can be considered:

- jurisdictions identified by FATF or FSRBs as high risk or with strategic deficiencies in AML/CFT;
- jurisdictions believed or known to have ineffective AML/CFT regimes;
- jurisdictions with impaired international cooperation;
- jurisdictions subject to international sanctions, embargoes, and restrictions;
- jurisdictions with high propensity for corruption listed on Transparency International's Corruption Perception Index, or from any other reliable source;
- countries' risk level listed on the Basel AML Index;
- jurisdictions that are believed or known to have strong links to terrorist funding, groups or activities;
- jurisdictions that are politically unstable or are in political turmoil;
- jurisdictions identified as being tax havens by the Organisation for Economic Co-operation and Development (OECD); and
- jurisdictions that are materially associated with the production and/or transnational shipment of illicit narcotics and psychotropic substances.

When a Firm undertakes a risk assessment, it must consider the ML/TF risk with regard to the countries its customers are based in, and countries they conduct their business in or through, as well as any overseas institutions that it may deal with. In relation to customers having dual nationalities, consideration must be given for the higher risk nationality that the customer possesses (if applicable).

A key FATF objective is to continually identify jurisdictions with weak or strategically deficient AML/CFT regimes. Such jurisdictions fall into two groups:

a. Those where enhanced due diligence measures should be applied,

proportionate to the risks arising from the identified deficiencies; and

b. Those where there are serious, longstanding, strategic deficiencies which require the application of countermeasures, in addition to enhanced due diligence measures.

FATF maintains lists of such jurisdictions, known as High Risk and Other Monitored Jurisdictions (HROMJs). The lists are updated in February, June, and October each year. Firms are strongly advised to monitor the lists and use them as part of their ongoing assessment of jurisdiction risk, and apply the findings and conclusions in their operational processes.

FATF reports are a good starting point to commence and update an assessment of a specific jurisdiction. The best sources of information on supervision and regulation are the Mutual Evaluations undertaken by FATF and FSRBs, IMF, and the World Bank. These provide granular information about a jurisdiction's technical compliance standards, and about the effectiveness of their implementation effort. Due to the scoring methodology used by FATF, it is possible that a jurisdiction may perform poorly or moderately on certain elements of the Mutual Evaluation, yet not be listed as a HROMJ as their overall score does not merit such listing. Therefore, Firms need to look beyond FATF's listing process and consider the nature of a jurisdiction's weaknesses, and factor those into their jurisdictional risk rating process.

The reputation of the country is another important factor to consider. Other international organisations regularly publish reports on perceived crime and corruption levels in countries.

B. United Nations sanctions and embargoes, and domestic NCTC designated sanctioned individuals and entities

United Nations sanctions and embargoes are financial, political, and trade restrictions put in place against target countries with the aim of maintaining or restoring international peace and security. The main aim of all UN sanctions and embargoes is to implement decisions by its Security Council.

Countries listed for the following are generally considered higher risk countries, and must be factored into country risk assessments by Firms.

- Arms embargoes
- Embargoes for nuclear proliferation
- Financial sanctions and asset freezes
- Travel bans
- Prohibited activities
- Import and export restrictions

The State of Qatar also maintains a domestic list of sanctioned individuals and entities.

All Firms are obligated to ensure that they have appropriate arrangements in place to screen customers and jurisdictions against the United Nations and NCTC lists of sanctions and embargoes, as a minimum. Refer to the guidance on CDD for further details on screening.

C. Other international sanctions

Economic and trade sanctions have been imposed by countries and international bodies to target some foreign countries, terrorists, drug traffickers, and those involved with the proliferation of weapons of mass destruction. Firms should also be aware of other sanctions that are relevant to their operations and areas of business. For example, unilateral sanctions by the United States in some cases impose secondary sanctions on third-country Firms transacting with sanctioned parties or otherwise conducting business that would be subject to the sanctions requirements if undertaken by US entities. Sanctions risk is a major driver of recent "de-risking" activity. Given the critical nature of US Dollar-denominated correspondent banking relationships to international trade, knowledge of US sanctions can be particularly relevant.

Refer to **Appendix 4** for resources to assist in the assessment of countries.

APPENDIX 1 - EXAMPLE PROCESS FOR A BUSINESS RISK ASSESSMENT

The examples serve to illustrate parts of a risk assessment methodology that could be applied by a Firm, however, the Firm should fully document their approach for arriving at risk ratings within their Threat Assessment Methodology. The examples provided are neither exhaustive nor binding.

1. Define the inherent risk factors.
2. Weight the inherent risk factors as per methodology.
3. Collect the data and subject it to appropriate review.
4. Score the inherent risk factors to arrive at both.
   a. an individual risk category rating, e.g. High, Moderate, Low (HML); and
   b. an overall HML score.
5. Define the control effectiveness categories.
6. Identify all the controls and map either to:
   a. the controls categories:
      i. Weight the categories based on importance, number of controls, number of key controls; and
      ii. Score the control effectiveness by aggregating the results to get an overall HML score; or
   b. the Inherent risk categories:
      i. Weight the controls based on importance, key controls.
      ii. Map the controls to each of the inherent risk categories and score those controls in aggregate against each risk category; and
      iii. Aggregate the control effectiveness categories to get an overall HML score;
7. Note and record the shortcomings or weaknesses in each of the identified controls for future remediation work (see 10 below);
8. Take the overall inherent risk score and apply the effectiveness of the controls;
9. Arrive at the residual risk and determine at the appropriate governance body whether the residual risk is within the Firm's tolerance or risk appetite; and
10. Determine the remediation action plan covering those items in 8 above that are determined as being in need of further action, by whom and by when.

APPENDIX 2: THREAT FACTORS CLASSIFICATION

Threat factors	Low threat	Medium threat	High threat
Availability and accessibility The availability and accessibility of products or services that might be misused for ML/TF	**Difficult** Difficult to access and/or may cost more than other options.	**Moderate** Reasonably accessible and/or a financially viable option.	**Easy** Widely accessible and available via a number of means and/or relatively low cost.
Ease of use Knowledge and/or technical expertise and support required	**Difficult** Requires more planning, knowledge and/or technical expertise than other options.	**Moderate** Requires moderate levels of planning, knowledge and/or technical expertise.	**Easy** Relatively easy to abuse; little planning, knowledge and/or technical expertise required compared to other options.
Deterrence The existence, adequacy, and effectiveness of controls and/or other barriers to abuse	**Significant** Deterrence measures and controls exist and are reasonably effective at deterring ML/TF.	**Limited** Deterrence measures and controls have some effect in deterring criminal abuse of the service.	**Weaker** There are limited or no measures and controls in place, or they are not working as intended.

Detection The existence, adequacy, and effectiveness of mechanisms for ML/TF to be identified and reported to authorities	**Likely** A range of money laundering methods is visible and likely to be detected.	**Limited** Some money laundering methods may be visible but limited reporting, high volumes of funds flows and/or effective evasion techniques limits detection.	**Difficult** Detection is difficult and there are few financial or other indicators of suspicious activity.
Intent The perceived attractiveness of ML/TF through this institution	**Low** Perceived as relatively unattractive and/or insecure.	**Moderate** Perceived as moderately attractive and/or fairly secure.	**High** Perceived as attractive and/or secure.

APPENDIX 3: SCORING OF RISK FACTORS

1. Scoring of Customer Risk

In scoring customer risk, Firms may wish to take into account the following examples of customer business relationship scenarios that may have a bearing on how a risk is scored. The following is an example only, and Firms may have additional and/or more specific business relationships and scenarios to consider. Similarly, Firms may impose a risk score (and weight) that is appropriate to the perceived risk that the customer business relationship may pose. The examples and scoring numbers provided are neither exhaustive nor binding.

Customer business relationship scenarios (example)	Score
Customer involved in a complex business ownership structure with no legitimate commercial rationale.	10
Customer that is a legal person (trust, company or other legal arrangement) has a complex business structure with little commercial justification, which obscures the identity of UBOs of the customer.	10
Customer is in a position that may expose them to corruption.	9
Customer is engaged in a cash intensive business.	7
Customer is a PEP.	9
Source of funds and wealth is difficult to verify.	9
There is no commercial rationale for a customer buying the products that it seeks, or the customer requests undue levels of secrecy.	10
BOs of a legal person are difficult to identify and/or verify.	9
There is a one-off transaction in comparison with an ongoing business relationship or series of transactions.	8

Customer makes or accepts payments (for example electronic transfers) to or from accounts that have not been identified by the firm.	10
Customer, when migrating from one product or service to another, carries a different type and level of ML/TF risk.	5
Customer has income which is not employment-based or from a regular known source.	8
Customer is new rather than having a long- term and active business relationship with the Firm.	5
Customer is an unregistered charity, foundation or cultural association.	10
Customer has a dual nationality, and at least one is from a high risk jurisdiction.	10

Note, the risk rating of a customer will affect the intensity of the CDD level. Refer to the CDD guidance for more information.

2. Scoring for Product Risk

The product risk scoring will be driven by the range and type of products that a Firm offers in relation to the nature of the business relationship with customers. The examples and scoring numbers provided are neither exhaustive nor binding.

In scoring product risk, Firms may wish to take into account the following examples of characteristics of products which may have a bearing on how a risk is scored. The following is an example only, and Firms may have additional products and scenarios to consider. Similarly, Firms may impose a risk score (and weight) that is appropriate to the perceived risk that the product may pose.

Product risk scenarios (example)	Score
Ability to make payments to third parties	6
Ability to pay in or withdraw cash	6
Ability to migrate from one product to another	5
Ability to use numbered accounts	9
Ability to pool underlying customers	9
There is no clear commercial rationale for the customer seeking the product or service	10
An undue level of secrecy is requested regarding a product or service	10
Products/services provided to the customer are primarily of a private banking and/or wealth management kind	7

3. Scoring for Interface Risk

Interface risk scoring will be driven by the mechanisms used to start or conduct business relationships with customers.

In scoring interface risk, Firms may wish to take into account the following examples of interface scenarios which may have a bearing on how a risk is scored. The following is an example only and Firms may have additional distribution channels and scenarios to consider. Similarly, Firms may impose a risk score (and weight) that is appropriate to the perceived risk that any interface may pose. The examples and scoring numbers provided are neither exhaustive nor binding.

Interface risk scenarios (example)	Score
Indirect relationship with the customer – where reliance is placed on third parties or intermediaries to undertake CDD	7
Customer makes withdrawal, transfer or drawdown instructions by phone or fax	6
Business relationships conducted through the post	5
Business relationships conducted solely over the Internet	10
Services and transactions provided or conducted over the Internet, using ATMs or by telephone or fax	8
Electronic point of sale transactions using prepaid, reloadable or account-linked value cards	8

4. Scoring for Jurisdiction Risk

Jurisdiction risk scoring will be driven by the types of jurisdictions where a business relationship with a customer is associated.

In scoring jurisdiction risk, Firms may wish to take into account the following examples of jurisdiction factors which may have a bearing on how a risk is scored. More generally, Jurisdiction (Country) risk, in conjunction with other risk factors, provides useful information when assessing ML and TF risks. Factors that may result in a determination that a jurisdiction poses a higher risk are included in the scenario. The following is an

example only and Firms may have additional jurisdictional risks and scenarios to consider. Similarly, Firms may impose a risk score (and weight) that is appropriate to the perceived risk that any jurisdictional risk may pose. Please refer to the section on higher risk countries. The examples and scoring numbers provided are neither exhaustive nor binding.

Jurisdiction risk scenarios (example)	Score
Customer is based in, or conducting business through or in, a high-risk jurisdiction and/or a jurisdiction known to suffer from corruption	9
Beneficial owners of a legal person are resident in a high-risk jurisdiction	8
Customer makes or accepts payments (for example, electronic transfers) to or from offshore accounts	6
Customer has access to offshore funds (for example, cash withdrawal or electronic funds transfer)	6
Customer's business is registered in a foreign jurisdiction with no local operations	8
Customer is represented by another person in another jurisdiction, such as under a power of attorney	7
Countries identified by FATF Statements as having weak AML/CFT regimes, and for which financial institutions should give special attention to business relationships and transactions	9

Countries or geographic areas subject to sanctions, embargoes, or statements of concern issued by international bodies such as the United Nations, FATF, or governments. In addition, in some circumstances, countries subject to sanctions or measures similar to those issued by bodies such as the United Nations, but which may not be universally recognised, may be given credence by a product provider or intermediary because of the standing of the issuing body and the nature of the measures	10
Countries or geographic areas identified by credible sources as lacking appropriate AML/ CFT laws, regulations and other measures	10
Countries or geographic areas identified by credible sources as providing funding or support for terrorist activities or that have designated terrorist organisation operating within them	10
Countries or geographic areas identified by credible sources as having significant levels of corruption, or other criminal activity	9
Countries or geographic areas where protection for customer privacy prevents the effective implementation of AML/CFT requirements and/or facilitates the framework for the establishment of shell-companies or the issuance of bearer shares and/or prevent effective information sharing and international cooperation	9
Cross border elements such as the product provider, the customer and the beneficiary of the contract being in separate jurisdictions	8

APPENDIX 4: RESOURCES ON COUNTRY ASSESSMENT

The hyperlinks below are provided for convenience, and may be subject to change without notice by the relevant website owners.

United Nations Security Council
https://www.un.org/sc/suborg/en/

United Nations Sanctions
https://www.un.org/sc/suborg/en/sanctions/information

Wolfsberg Group
Country Risk Frequently Asked Questions (FAQs) 2018
https://www.wolfsberg-principles.com/sites/default/files/wb/Wolfsberg%20FC%20Country%20Risk%20FAQs%20Mar18.pdf

Basel AML Index
2019 Report
https://www.baselgovernance.org/sites/default/files/2019-08/Basel%20AML%20Index%202019.pdf

Financial Action Task Force
High-risk and non-cooperative jurisdictions
http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/?hf=10&b=0&s=desc(fatf_releasedate)

Financial Action Task Force
Improving Global AML/CFT Compliance: On-going Process
18 October 2019
http://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/public-statement-october-2019.html
http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/documents/fatf-compliance-june-2017.html

Financial Markets Authority – New Zealand
Countries Assessment Guideline
https://www.rbnz.govt.nz/-/media/ReserveBank/Files/regulation-and-supervision/anti-money-laundering/guidance-and-publications/4853287.pdf?la=en

Organisation for Economic Co-operation and Development
List of Unco-operative Tax Havens
http://www.oecd.org/countries/monaco/listofunco-operativetaxhavens.htm

The Financial Secrecy Index
https://www.financialsecrecyindex.com/introduction/fsi-2018-results

Transparency International
Corruption Perception Index 2018
https://www.transparency.org/files/content/pages/2018_CPI_Executive_Summary.pdf

European Union Sanctions
https://www.sanctionsmap.eu/#/main?search=%7B%22value%22:%22%22,%22searchType%22:%7B%22id%22:1,%22title%22:%22regimes,%20persons,%20entities%22%7D%7D

World Bank World Governance Indicators
http://info.worldbank.org/governance/wgi/#home

Fragile States Index
http://fundforpeace.org/fsi

Global Terrorism Database
https://www.start.umd.edu/gtd/

The Government of UK – guidance on sanctions, embargoes and restrictions
March 2016
https://www.gov.uk/guidance/sanctions-embargoes-and-restrictions

RESOURCES

The hyperlinks below are provided for convenience, and may be subject to change without notice by the relevant website owners.

Basel Committee on Banking Supervision
Guidelines - Sound management of risks related to money laundering and financing of terrorism
June 2017
http://www.bis.org/bcbs/publ/d405.pdf

Financial Action Task Force
The 40 Recommendations
June 2017
http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

Financial Action Task Force
FATF Guidance – National Money Laundering and Terrorist Financing Risk Assessment
http://www.fatf-gafi.org/media/fatf/content/images/National_ML_TF_Risk_Assessment.pdf

Financial Action Task Force
Global Money Laundering & Terrorist Financing Threat Assessment
July 2010
http://www.fatf-gafi.org/media/fatf/documents/reports/Global%20Threat%20assessment.pdf

Investment Management, Association of Singapore
Guidance to Assessing Money Laundering and Financing of Terrorism (ML/FT) Risk
http://www.imas.org.sg/uploads/media/2015/12/01/1026_IMAS_Guidance_to_assessing_ML-TF_v2.pdf

Monetary Authority of Singapore
Guidelines to MAS Notice 626 on prevention of money laundering and countering the financing of terrorism
April 2015
http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Anti_Money%20Laundering_Countering%20the%20Financing%20of%20Terrorism/Guidelines%20to%20MAS%20Notice%20626%20%20April%202015.pdf

Reserve Bank of New Zealand
Risk Assessment Guideline
https://fma.govt.nz/assets/Guidance/_versions/3234/110613-aml-cft-risk-assessment-guideline.1.pdf

Wolfsberg Group
Frequently Asked Questions on Risk Assessments for Money Laundering, Sanctions and Bribery & Corruption
http://www.wolfsberg-principles.com/pdf/faq/Wolfsberg-Risk-Assessment-FAQs-2015.pdf