Guidance on
The Risk-Based Approach
**TABLE OF CONTENTS**

Glossary of Terms ............................................................................................................... 3  
1. Purpose ............................................................................................................................. 4  
2. Risk Management Framework .......................................................................................... 5  
3. Developing the AML/CFT Programme ............................................................................. 6  
4. Independent Review and Testing ...................................................................................... 6  
5. PART A - Guidance on the Risk-Based Approach ............................................................ 7  
   A. The Business Risk Assessment ....................................................................................... 8  
   B. Threat Assessment Methodology ................................................................................. 18  
   C. Risk Profiling of Business Relationships .................................................................... 20  
6. PART B - Guidance on Higher Risk Countries ................................................................. 23  
7. Appendix 1 - Example Process for a Business Risk Assessment ....................................... 25  
8. Appendix - 2 Threat Factors Classification ................................................................... 26  
9. Appendix 3 - Scoring of Risk Factors ............................................................................ 28  
   A. Scoring of Customer Risks ......................................................................................... 28  
   B. Scoring for Product Risk ............................................................................................ 29  
   C. Scoring for Interface Risk .......................................................................................... 30  
   D. Scoring for Jurisdiction Risk ...................................................................................... 31  
10. Appendix 4 - Resources on Country Assessment ........................................................... 33  
11. Resources ......................................................................................................................... 35  

Version control:  
Guidance on the Risk-Based Approach  
V3.0  
May 2018
GLOSSARY OF TERMS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABC</td>
<td>Anti-bribery and Corruption</td>
</tr>
<tr>
<td>AML/CFT</td>
<td>Anti-Money Laundering/Combatting Terrorist Financing</td>
</tr>
<tr>
<td>AML/CFTR</td>
<td>State of Qatar AML/CFT Law</td>
</tr>
<tr>
<td>AMLG</td>
<td>State of Qatar AML/CFT Law</td>
</tr>
<tr>
<td>BO</td>
<td>Beneficial Owner</td>
</tr>
<tr>
<td>CDD</td>
<td>Customer Due Diligence</td>
</tr>
<tr>
<td>DNFBP</td>
<td>Designated Non-Financial Business or Profession</td>
</tr>
<tr>
<td>FATF</td>
<td>Financial Action Task Force</td>
</tr>
<tr>
<td>FI</td>
<td>Financial Institution</td>
</tr>
<tr>
<td>FIRM</td>
<td>Financial Institution and Designated Non-Financial Business or Profession</td>
</tr>
<tr>
<td>KYC</td>
<td>Know Your Customer</td>
</tr>
<tr>
<td>ML</td>
<td>Money Laundering</td>
</tr>
<tr>
<td>PEP</td>
<td>Politically Exposed Person</td>
</tr>
<tr>
<td>QFCRA</td>
<td>Qatar Financial Centre Regulatory Authority</td>
</tr>
<tr>
<td>TF</td>
<td>Terrorist Financing</td>
</tr>
<tr>
<td>UBO</td>
<td>Ultimate Beneficial Owner</td>
</tr>
</tbody>
</table>
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 legislation¹ applicable in the State of Qatar or the Qatar Financial Centre. Firms remain responsible for compliance with legislation which is relevant to their operations.

This guidance is intended to assist Firms 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, 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 (PART A); and
- guidance and information to assist Firms on dealing with higher risk countries (PART B).

¹ The term “legislation” is used 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 risk-based approach is adopted to identify, mitigate and manage money laundering and terrorist financing risks.

Firms must develop a programme against ML and TF. Firms are best placed to assess ML/TF risk(s) they may reasonably face in conducting business, having regard to their business (size, nature and complexity). 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 the 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 risk-based approach relevant to a firm’s business and circumstances should assist the Firm to manage ML/TF risks it may face.

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

**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 are required to develop a programme against ML and TF. Firms should have particular focus on the key requirements of the relevant rules and legislations that constitute the building blocks for developing and implementing the programme. The senior management of a Firm is to ensure that the Firm’s policies, procedures, systems and controls appropriately and adequately address the requirements of the Rules and the legislation.

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

Firms operating in the Qatar Financial Centre (QFC) must retain relevant records for at least six years. All other Firms operating in the State of Qatar must retain relevant records for at least five 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 it is commensurate with the nature, scale and complexity of the Firm and whether it remains fit for purpose.
PART A – GUIDANCE ON THE RISK-BASED APPROACH

In line with FATF recommendation 1 (and other relevant recommendations and interpretative notes) and the relevant legislation and rules, Firms are required to adopt a risk-based approach. The risk-based approach 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 risk-based approach allows Firms to allocate 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 customer 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. Ideally, 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 financiers 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 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

A Firm must be able to demonstrate that it has considered the exposure of the business to ML/TF risks. The Business Risk Assessment must be documented, receive senior management’s approval and be reviewed at periodic intervals, at a minimum on an annual basis.

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.

1. What is the purpose of a risk assessment?

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

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, 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 the 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 the 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 the action plan, 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 or
the jurisdictions it deals with or external triggers such as the deployment of a major
sanctions program or changes in applicable laws and regulations.

Regardless of the frequency of risk assessments, Firms are usually required to report
annually (such as the Annual MLRO Report) on the status 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, the criteria used to score, 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 may not be the norm, 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 compliance, or
whether it is an integrated risk assessment, capturing issues identified by both business
and compliance.

Some Firms will have a dedicated AML/Financial Crime Compliance department
responsible for AML, CFT, Sanctions, Anti-bribery and Corruption (“ABC”) in addition to
other financial crime prevention, for which the risk assessment scope will be broad
and inclusive. Yet other Firms will have standalone units to deal with AML, CFT,
Sanctions and ABC in addition to other financial crime prevention, which may result
in segregated risk assessments.

Regardless of whether a Firm formally evaluates all financial crime risks through the
ML/TF risk assessment or through separate assessment processes, the Firm’s senior management and MLRO are responsible and accountable for understanding the extent of the risks posed across the Firm. Similarly, 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 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 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 senior management of a Firm 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 of their ML/TF risks, Firms need to consider the following:

- the example of a QFC Threat Matrix (see Figure 1) and the threats and risks identified in the national-level risk assessment;
- 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
operation;

- 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 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 are the steps to a Business Risk Assessment?**

- **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, bribery and corruption in the absence of any control environment being applied. A Firm’s approach to categorising risks should be clearly documented.

a) **Customers**

b) **Products and Services**

c) **Interface**

d) **Jurisdictions**

e) **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 in a through e—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 financial crime.

Managing the risk factors inadequately could lead to the Firm being exploited for ML or TF, which in turn could drive reputational harm, regulatory penalties, 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 risk-based approach 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.

a. 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, 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 amount of ML/TF risk each type carries. For the business division, unit or business line in question, the volume (#) 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 risk classification, e.g. low, moderate, high and higher risk, in order to determine the overall inherent customer risk.

b. 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 (for example, low, moderate, high or higher) 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 volume (#) 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, high and higher risk, in order to determine the overall inherent product risk.
c. Interface/ delivery
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 though 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, high and higher risk, in order to determine the overall inherent channels risk.

d. 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 involving 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, 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 from 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 which 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 ABC risk assessment. 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 Part B – Guidance on Higher Risk Countries.

e. 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 or changed. The main "Other Qualitative Risk Factors" might include:

- customer base stability;
- integration of IT systems;
- expected account/customer growth;
- expected revenue growth;
- recent AML Compliance 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;
- 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.

\[
\text{Inherent risk score} - \text{Controls score} = \text{Residual risk}
\]

The residual risk score then needs to be tied to a risk rating - high, medium and low, which is the standard 3 tier rating scale. Firms can also implement a 5 tier rating scale - high, medium high, medium, medium low and low. Firms need to use a scale which best suits their businesses.
The residual risk is an important measurement which 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 which reflects the associated level of risk. Each risk area may then be assigned a weight which reflects the level of importance in the overall risk calculation relative to other risk areas.

Similarly, each control may be assigned a weight which 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.

8. **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 which are prioritised appropriately and tracked centrally. Ownership of these actions may be allocated to different parts of the business but Compliance 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 are 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.

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.

9. **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. 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 are important aspects 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 following example of a threat matrix (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 towards 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.
C. 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. Refer to the guidance on CDD.

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:

a. customer risk
b. product risk
c. interface risk
d. jurisdiction risk

Each risk factor is usually assigned a score which reflects the associated level of risk. Each risk factor may then be assigned a weight which 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 the scoring risk appendices, 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 shows an example where the proposed business relationship profile is within the Firm’s risk appetite. In this case the Firm will need to perform basic due diligence.

Figure 2 – Example of risk profiling where the customer profile fits with 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.
Risk profile of customers

"Acceptable" risk profile of firm

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 transact this business, or, by conducting additional due diligence checks on the customer, decide to accept it.

Refer to Appendix 3 for risk scoring of business relationships
6. PART B - GUIDANCE ON HIGHER RISK COUNTRIES

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 countemasures when called upon to do so by the FATF. Countries should also be able to apply countemasures independently of any call by the FATF to do so. Such countemasures 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 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 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).

FATF publishes a list of high risk and non-cooperative jurisdictions. FATF also identifies jurisdictions with weak measures to combat ML/TF. Firms are advised to check the FATF website frequently for updates on high risk countries and to implement amendments to their Business Risk Assessment and risk scoring processes in response to changes in countries’ status.

FATF reports are a good starting point to commence and update a country
assessment. The best sources of information on supervision and regulation for particular countries are the mutual evaluations undertaken by FATF and FATF-style regional bodies, IMF and the World Bank. There are practical limits on the number of detailed assessments these bodies can carry out in a given year. Jurisdictions that perform poorly on only a few elements of their FATF mutual evaluation will not necessarily rise to the FATF’s lists, although their deficiencies in these areas could elevate their risk. Consequently, the FATF’s lists, while an important component of jurisdictional risk rating, cannot be the sole criterion a Firm uses to risk-rate jurisdictions.

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.

**United Nations sanctions and embargoes**

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 in while conducting a country risk assessment.

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

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

**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 which 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 sanctioned 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.
7. **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

<table>
<thead>
<tr>
<th>Threat factors</th>
<th>Low threat</th>
<th>Medium threat</th>
<th>High threat</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Availability and accessibility</strong>&lt;br&gt;The availability and accessibility of products or services that might be misused for ML/TF</td>
<td><strong>Difficult</strong>&lt;br&gt;Difficult to access and/or may cost more than other options.</td>
<td><strong>Moderate</strong>&lt;br&gt;Reasonably accessible and/or a financially viable option.</td>
<td><strong>Easy</strong>&lt;br&gt;Widely accessible and available via a number of means and/or relatively low cost.</td>
</tr>
<tr>
<td><strong>Ease of use</strong>&lt;br&gt;Knowledge and/or technical expertise and support required</td>
<td><strong>Difficult</strong>&lt;br&gt;Requires more planning, knowledge and/or technical expertise than other options.</td>
<td><strong>Moderate</strong>&lt;br&gt;Requires moderate levels of planning, knowledge and/or technical expertise.</td>
<td><strong>Easy</strong>&lt;br&gt;Relatively easy to abuse; little planning, knowledge and/or technical expertise required compared to other options.</td>
</tr>
<tr>
<td><strong>Deterrence</strong>&lt;br&gt;The existence, adequacy, and effectiveness of controls and/or other barriers to abuse</td>
<td><strong>Significant</strong>&lt;br&gt;Deterrence measures and controls exist and are reasonably effective at deterring ML/TF.</td>
<td><strong>Limited</strong>&lt;br&gt;Deterrence measures and controls have some effect in deterring criminal abuse of the service.</td>
<td><strong>Weaker</strong>&lt;br&gt;There are limited or no measures and controls in place, or they are not working as intended.</td>
</tr>
<tr>
<td><strong>Detection</strong>&lt;br&gt;The existence, adequacy, and effectiveness of mechanisms for ML/TF to be identified and reported to authorities</td>
<td><strong>Likely</strong>&lt;br&gt;A range of money laundering methods is visible and likely to be detected.</td>
<td><strong>Limited</strong>&lt;br&gt;Some money laundering methods may be visible but limited reporting, high volumes of funds flows and/or effective evasion techniques limits detection.</td>
<td><strong>Difficult</strong>&lt;br&gt;Detection is difficult and there are few financial or other indicators of suspicious activity.</td>
</tr>
<tr>
<td><strong>Intent</strong>&lt;br&gt;The perceived attractiveness of ML/TF through this institution</td>
<td><strong>Low</strong>&lt;br&gt;Perceived as relatively unattractive and/or insecure.</td>
<td><strong>Moderate</strong>&lt;br&gt;Perceived as moderately attractive and/or fairly secure.</td>
<td><strong>High</strong>&lt;br&gt;Perceived as attractive and/or secure.</td>
</tr>
</tbody>
</table>
## 9. APPENDIX 3 – SCORING OF RISK FACTORS

### A. SCORING OF CUSTOMER RISKS

In scoring customer risk, Firms may wish to take into account the following examples of customer business relationship scenarios which 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.

<table>
<thead>
<tr>
<th>Customer business relationship scenarios</th>
<th>Score 1-10 (Example)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer involved in a complex business ownership structure with no legitimate commercial rationale.</td>
<td>10</td>
</tr>
<tr>
<td>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.</td>
<td>10</td>
</tr>
<tr>
<td>Customer is in a position which may expose them to corruption.</td>
<td>9</td>
</tr>
<tr>
<td>Customer is engaged in a cash intensive business.</td>
<td>7</td>
</tr>
<tr>
<td>Customer is a PEP.</td>
<td>9</td>
</tr>
<tr>
<td>Source of funds and wealth is difficult to verify.</td>
<td>9</td>
</tr>
<tr>
<td>There is no commercial rationale for a customer buying the products that it seeks, or the customer requests undue levels of secrecy.</td>
<td>10</td>
</tr>
<tr>
<td>BOs of a legal person are difficult to identify and/or verify.</td>
<td>9</td>
</tr>
<tr>
<td>There is a one-off transaction in comparison with an ongoing business relationship or series of transactions.</td>
<td>8</td>
</tr>
</tbody>
</table>
Customer makes or accepts payments (for example electronic transfers) to or from accounts which 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.

**B. 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.

<table>
<thead>
<tr>
<th>Product risk scoring scenarios</th>
<th>Score 1-10 (Example)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ability to make payments to third parties</td>
<td>6</td>
</tr>
<tr>
<td>Ability to pay in or withdraw cash</td>
<td>6</td>
</tr>
<tr>
<td>Ability to migrate from one product to another</td>
<td>5</td>
</tr>
<tr>
<td>Ability to use numbered accounts</td>
<td>9</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---</td>
</tr>
<tr>
<td>Ability to pool underlying customers</td>
<td>9</td>
</tr>
<tr>
<td>There is no clear commercial rationale for the customer seeking the product or service</td>
<td>10</td>
</tr>
<tr>
<td>An undue level of secrecy is requested regarding a product or service</td>
<td>10</td>
</tr>
<tr>
<td>Products/services provided to the customer are primarily of a private banking and/or wealth management kind</td>
<td>7</td>
</tr>
</tbody>
</table>

C. 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.

<table>
<thead>
<tr>
<th>Scoring interface risk scenario</th>
<th>Score 1-10 (Example)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indirect relationship with the customer - where reliance is placed on third parties or intermediaries to undertake CDD</td>
<td>7</td>
</tr>
<tr>
<td>Customer makes withdrawal, transfer or drawdown instructions by phone or fax</td>
<td>6</td>
</tr>
<tr>
<td>Business relationships conducted through the post</td>
<td>5</td>
</tr>
<tr>
<td>Business relationships conducted solely over the Internet</td>
<td>10</td>
</tr>
</tbody>
</table>
D. 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.

<table>
<thead>
<tr>
<th>Jurisdiction interface risk factors scenarios</th>
<th>Score 1-10 (Example)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer is based in, or conducting business through or in, a high-risk jurisdiction and/or a jurisdiction known to suffer from corruption</td>
<td>9</td>
</tr>
<tr>
<td>Beneficial owners of a legal person are resident in a high-risk jurisdiction</td>
<td>8</td>
</tr>
<tr>
<td>Customer makes or accepts payments (for example, electronic transfers) to or from offshore accounts</td>
<td>6</td>
</tr>
<tr>
<td>Customer has access to offshore funds (for example, cash withdrawal or electronic funds transfer)</td>
<td>6</td>
</tr>
<tr>
<td>Customer’s business is registered in a foreign jurisdiction with no local operations</td>
<td>8</td>
</tr>
<tr>
<td>Country Feature</td>
<td>Relevant Page</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Customer is represented by another person in another jurisdiction, such as under a power of attorney</td>
<td>7</td>
</tr>
<tr>
<td>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</td>
<td>9</td>
</tr>
<tr>
<td>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</td>
<td>10</td>
</tr>
<tr>
<td>Countries or geographic areas identified by credible sources as lacking appropriate AML/CFT laws, regulations and other measures</td>
<td>10</td>
</tr>
<tr>
<td>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</td>
<td>10</td>
</tr>
<tr>
<td>Countries or geographic areas identified by credible sources as having significant levels of corruption, or other criminal activity</td>
<td>9</td>
</tr>
<tr>
<td>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</td>
<td>9</td>
</tr>
<tr>
<td>Cross border elements such as the product provider, the customer and the beneficiary of the contract being in separate jurisdictions</td>
<td>8</td>
</tr>
</tbody>
</table>
10. 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

United Nations Sanctions

Wolfsberg Group
Country Risk Frequently Asked Questions (FAQs) 2018

Basel AML Index
2016 Report

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
23 June 2017

Financial Markets Authority – New Zealand
Countries Assessment Guideline

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

Transparency International
Corruption Perception Index 2016

European Union Sanctions
https://www.sanctionsmap.eu/#/main?search=%7B%22value%22:%22%22,%22searchType%22:%7B%22%7B%22id%22:1,%22title%22:%22regimes%0Apersons%0Aentities%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
11. 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

**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

**Investment Management, Association of Singapore**
Guidance to Assessing Money Laundering and Financing of Terrorism (ML/FT) Risk

**Monetary Authority of Singapore**
Guidelines to MAS Notice 626 on prevention of money laundering and countering the financing of terrorism
April 2015

**Reserve Bank of New Zealand**
Risk Assessment Guideline
Wolfsberg Group
Frequently Asked Questions on Risk Assessments for Money Laundering, Sanctions and Bribery & Corruption