Board Paper No : 2024/301/09//S

Board Meeting No : 77 **Date** : 27/09/2024

LANKA CREDIT AND BUSINESS FINANCE PLC

MONEY LAUNDERING

&

TERRORIST FINANCING (ML/TF) RISK ASSESSMENT METHODOLOGY

Owner - Compliance Department
Approval – Board of Directors
Date of Approval – 27/09/2024

1. Money Laundering and Terrorism Financing (ML/TF) Risk Assessment

Purpose of the ML/TF Risk Assessment

Risk management is the process of identifying risk and developing policies and processes to minimize and manage risk. This requires the development of a process to identify, assess, prioritise, mitigate, manage and monitor risk exposures.

Money laundering (ML) or terrorist financing (TF) risk is the risk that an organization, or a product or service offered by an organization, may be used to facilitate ML/TF.

It is unrealistic that an organization would operate in a completely risk-free environment in terms of ML/TF. Therefore, an organization should identify the ML/TF risks it may reasonably face, then assess the best approach to reduce and manage those risks.

ML/TF risk assessment is a process of assessing an organisation's risk of, and vulnerabilities to, being used by money launderers and terrorist financiers.

To ensure completeness, consistency and accuracy of the assessment of ML/TF risks this ML/TF risk assessment methodology forms part of the AML Program / Policy.

2. ML/TF Risk Assessment Methodology

General

The methodology has been designed to identify and assess ML/TF risks by responding to a series of pre-defined questions, which generate an enterprise level ML/TF risk assessment.

Once ML/TF risks have been identified and assessed, it is the responsibility of the organization to develop, operationalize and continually monitor mitigating systems, processes and controls to effectively manage ML/TF risks.

These mitigating systems, processes and controls are set out in the AML Program and Customer Due Diligence Standards, which form part of the AML Program / Policy.

This ML/TF risk assessment methodology includes the following dimensions of ML/TF risk:

- Environmental Risk
    - Predicate offences;
    - Money laundering;
    - Terrorist financing;
    - Targeted financial sanctions; and
    - Regulatory compliance.

- Customer Risk
    - Customer type or legal form;
    - Politically exposed persons (PEPs);
    - Customer location; and
    - Customer business activities.

- Business Risk
    - Location of business operations;
    - Outsourced AML processes and controls; and
    - Employee risk.

- Channel Risk
    - Face to face customer engagement; and
    - Third party distribution channels.

- Product / Service Risk
    - Product or service characteristics and their vulnerabilities to ML/TF; and
    - Products / Services defined as higher ML/TF risk.

- Country Risk

This document explains how each risk factor within each of the risk categories is identified and assessed to determine the level of ML/TF risk. The document also provides definitions used as part of the ML/TF risk assessment.

Inherent and residual ML/TF risk

Both the inherent ML/TF risk and residual ML/TF risk are assessed for each risk category:

- Inherent ML/TF risk is the outcome of an assessment of the likelihood of a risk occurring and the impact of the risk, were it to occur. Inherent risk is the risk before controls are applied to mitigate the risk being assessed; and

- Residual ML/TF risk is the outcome of an assessment of the identified inherent risk after the existence and operational effectiveness of controls that have been put in place to mitigate that risk being assessed have been taken into consideration.

Inherent risk, control assessment and residual risk definitions

The definitions of inherent risk, control assessment and residual risk ratings are as follows:

Inherent Risk Rating (IRR)	
Significant	Major ML/TF risk. Effective controls are required to manage the risk.
High	Serious ML/TF risk. Effective controls are required to manage the risk.
Medium	Moderate ML/TF risk. Effective controls are required to reduce this risk if it is outside of the organisation's risk appetite.
Low	Minor or negligible ML/TF risk. Effective controls are should be considered to manage this risk in line with the organisation's risk appetite.

Control Assessment	
Excellent	Controls implemented where the design and performance have been determined to be highly effective at mitigating the risk.
Adequate	Controls implemented and the design and performance have been determined to be effective in mitigating the risk.
Poor	Controls implemented but either the design or performance have been determined to be ineffective in mitigating the risk.
Not Tested	Controls implemented but their design and performance have not been tested.
No Control	No controls have been implemented to mitigate the risk.

Residual Risk Rating (RRR)	
Significant	Risk almost sure to occur and/or risk presents major consequences.
High	Risk likely to occur and/or risk presents serious consequences.
Medium	Risk may occur and/or risk presents moderate consequences.
Low	Risk unlikely to occur and/or risk presents minor or negligible consequences.

3. Risk Assessment Results

The ML/TF risk assessment is structured on a number of levels.

Level	Description
Level 1	Executive Summary - One consolidated view of all the ML/TF risk at an organisation level.
Level 2	Risk Category - a consolidated view of the risk ratings for each of the following risk categories: • Environmental Risk • Customer Risk • Business Risk • Channel Risk • Product Risk Included is a summary of the inherent risk ratings, controls, and residual risk rating for each risk category and their sub-categories.
Level 3	Risk Sub-Category - a consolidated view of the risk rating of each of the risk sub-categories that make up a risk category.
Level 4	Individual Risk - a consolidated view of the risk rating of each risk component that make up a risk sub-category.
Level 5	Individual Risk - a detailed assessment of the risk, the risk's indicators, the inherent risk, the controls, the effectiveness of the controls and the residual risk rating for each risk assessed.

Consolidated risk ratings are calculated at level's 1, 2, 3 and 4 by assigning a numerical score to the rating results at the level below and aggregating those scores to determine the risk rating (refer to Risk Rating Aggregation section for more details).

The Model

The model includes the following categories, sub-categories and risks:

Risk Category	Risk Sub-Category	Individual Risk
Environmental Risk	Predicate Offence	Deceptive Crimes
		Illicit Trafficking
		Personal Crimes
		Property Crimes
	Money Laundering	Higher Risk Business Operations
		Higher Risk Channels
		Higher Risk Customer Transactions
		Higher Risk Customers
		Higher Risk Products and Services
	Terrorist Financing	Higher Risk Customer
		Higher Risk Customer Transactions
	Targeted Financial Sanctions	Higher Risk Customer
		Higher Risk Customer Transactions
	Regulatory Compliance	Governance & Oversight
		Program Alignment to ML/TF Risks
		Program Non-Compliance
		Reporting
Customer Risk	Customer Type Risk	Customer Legal Form Risk
		Customer PEP Risk
	Customer Footprint Risk	Customer Location Risk
		Customer Business Risk
Business Risk	Business Operations Risk	Business Location Risk
		Business Outsource Control Risk
	Business Employee Risk	Business Employee Screening Risk
		Business Employee Role Risk
Channel Risk	Non-Face-To-Face Risk	Channel Non-Face-To-Face Risk
	Third Party Use Risk	Channel Third Party Use Risk
		Channel Third Party Location
Product Risk*	Not Applicable*	Product 1*
		Product 2*
		Product 3*
		Product 4*
		Product 5*

* Note – the products and services relevant to the organisation are added and assessed individually at the time of the assessment so the number of products of products and services offered will determine the number of risk ratings in the product risk section.

Risk Rating Aggregation

At each level the risk ratings are aggregated as follows:

1) Each risk rating is assigned a value i.e. Low = 1, Medium = 2, High =3, Significant = 4;
2) The values of each relevant risk rating are summed and then divided by the number of relevant risk ratings to determine an average value;
3) The average value is then rounded up or down to the nearest integer to determine the average rating.

For example:

Product risk category has 3 products each with a risk rating:

Product 1 = Medium Product 2 = Medium Product 3 = High

The aggregated risk rating for product risk is therefore (2+2+3)/3=2.33=Medium

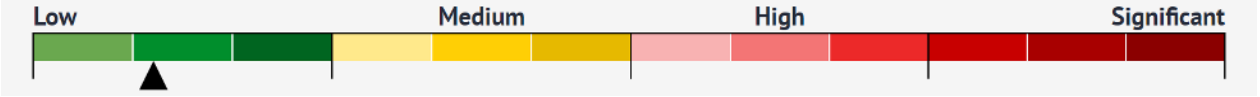
If the 3 products were rated as follows:

Product 1 = High Product 2 = Medium Product 3 = High

The aggregated risk rating for product risk is therefore (3+2+3)/3=2.66=High

The overall aggregated risk rating is calculated from the ratings of the risk categories.

The overall aggregated risk rating is shown as Low, Medium or High, but is also plotted on a scale such as the one below:



4. Environmental Risk

What is environmental risk?

Environmental risk considers the external and internal environments that an organisation operates in.

Predicate crimes that can give rise to ML/TF are considered. Based on international guidance, the organisation's vulnerability to these crimes is assessed. This vulnerability may be because a customer is involved in the commission of one or more predicate crimes and/or is seeking to use products and services to launder the proceeds of a predicate crime.

Predicate crimes have been grouped into several categories. The grouping includes deceptive crimes, illicit trafficking, property crimes, and crimes against the person (personal crimes).

The internal vulnerability of the organisation to being used to launder money, finance terrorism, or breach targeted financial sanctions is also considered.

In addition, the organisation's vulnerability to non-compliance with relevant law and regulation is also considered, should it not have appropriate controls or adequate responses to those obligations.

Environmental ML/TF risk is assessed at the inherent risk and residual risk level.

Environmental inherent risk

Inherent environmental ML/TF risks are assessed and rated by applying a combination of risk likelihood and risk impact, using the following matrix:

Environmental Inherent Risk Rating (IRR)		**Impact**			
		Minor	**Moderate**	**Major**	**Unknown**
Likelihood	**Very likely**	Medium	High	Significant	High
	Likely	Low	Medium	High	High
	Unlikely	Low	Low	Medium	High
	Unknown	High	High	High	High

The likelihood and impact ratings when assessing inherent environmental ML/TF risk are defined as follows:

Likelihood	
Very likely	Almost certain that the risk will occur several times a year based on it occurring more than once previously and being expected to occur more than once in the future.
Likely	High probability the risk will occur at least once based on it occurring previously and it being expected to occur again.
Unlikely	Low probability that the risk will occur based it having not occurred previously and not being expected to occur in the future.
Unknown	Insufficient knowledge or data to form a view on whether the risk will or could occur.
Impact	
Major	The risk occurring could result in significant financial penalties (with reference to the size and profitability of the organisation) and/ or result in limitations or restrictions on business activities which could affect the organisation's ability to continue as a going concern.
Moderate	The risk occurring could result in financial penalties and/or limitations or restrictions on business activities, but would not affect the organisation's ability to continue as a going concern.
Minor	The risk occurring may result in financial penalties, but these are unlikely to affect the organisation's ability to continue as a going concern.
Unknown	Insufficient knowledge or data to form a view on whether the risk would result in financial penalties and/or limitations or restrictions on business activities.

Additional contextual data

The following additional data that provides context to the risk of the environment is collected:

- The types of predicate offences that the organisation is vulnerable to;
- Whether the organisation is located in a geographical area that is recognized by authorities as being particularly vulnerable to predicate offences;
- Whether customers have been involved in any predicate offences;
- Orders or requests for information on any customers received from authorities in the last 12 months.

Environmental residual risk

Residual environmental ML/TF risks are assessed by overlaying the inherent ML/TF risk with an assessment of the controls to mitigate that risk, using the following matrix:

Environmental Residual Risk Rating (RRR)		Control Assessment			
		Excellent	**Adequate**	**Poor**	**No Control / Not Tested**
Environmental Inherent Risk Rating (IRR)	**Significant**	Medium	High	Significant	Significant
	High	Low	Medium	High	High
	Medium	Low	Low	Medium	Medium
	Low	Low	Low	Low	Low

5. Customer Risk

What is customer risk?

ML/TF customer risk considers the vulnerability that customers may be involved in money laundering or terrorist financing activities. ML/TF customer risk is significantly influenced by the nature and/or attributes of a customer.

Customer inherent risk

Customer inherent risk at an enterprise level is assessed through a combination of:

- Customer type risk; and
- Customer footprint risk.

Customer type risk

Customer type risk is a combination of what legal form customers are and whether customers are politically exposed persons (PEPs):

- The type of customer and the percentage of each customer type (including individuals) that have been identified, through customer due diligence, to represent a higher ML/TF risk contributes to rating the customer base as higher footprint ML/TF risk. The greater the percentage of customer types identified as high risk, in the customer base, the higher the risk rating.
- Politically Exposed Person (PEP) risk is a term used to describe someone entrusted with a prominent public function, such as a senior political figure, or an individual closely related to such a person. The definition of PEP also includes close associates of senior political figures, who have joint beneficial ownership of a legal entity or legal arrangement between them. Where customers are PEPs this contributes to rating the customer base as higher footprint ML/TF risk. The higher the percentage of PEP's in the customer base, the higher the risk rating.

Customer type risk is assessed using the following matrix:

Customer Type Risk		**Customer Politically Exposed Person (PEP) Risk**			
		High	**Medium**	**Low**	**Unknown**
Customer Legal Form Risk	**High**	High	High	Medium	High
	Medium	High	Medium	Medium	High
	Low	Medium	Medium	Low	High
	Unknown	High	High	High	High

Customer footprint risk

Customer footprint risk is a combination of customer location risk and business risk assessment:

- Customer location risk relates to where customers are located, based, or have a contact address. Where customers are overseas or in a higher ML/TF risk country it may contribute to rating the customer base as representing a higher footprint ML/TF risk. The higher the percentage of overseas customers in the customer base the higher the percentage in countries rated as high risk or restricted, the higher the customer location risk rating.
- Customer business risk relates to nature of business activities that the customers undertake or are engaged in, as some activities are inherently more vulnerable than others to ML/TF. Where customers are engaged in or are undertaking higher ML/TF risk business activity, this may contribute to rating the customer base as higher footprint ML/TFrisk. The higher the percentage of customers in higher risk business activities, the higher the risk rating.

Customer footprint risk is assessed using the following matrix:

Customer Footprint Risk		**Customer Business Risk**			
		High	**Medium**	**Low**	**Unknown**
Customer Location Risk	**High**	High	High	Medium	High
	Medium	High	Medium	Medium	High
	Low	Medium	Medium	Low	High
	Unknown	High	High	High	High

Additional contextual data

The following additional data that provides context to the customer risk is collected:

- Whether the customer base profile has significantly changed in the last 12 months; and
- If so, in what way.

The overall inherent customer ML/TF risk is assessed by applying a combination of customer footprint risk and customer type risk, using the following matrix:

Customer Inherent Risk Rating (IRR)		Customer Type Risk		
		High	**Medium**	**Low**
Customer Footprint Risk	**High**	Significant	High	Medium
	Medium	High	Medium	Medium
	Low	Medium	Medium	Low

Customer residual risk

Residual customer ML/TF risks, are assessed by overlaying the inherent ML/TF risk with an assessment of the controls to mitigate that risk, using the following matrix:

Customer Residual Risk Rating (RRR)		Control Assessment			
		Excellent	**Adequate**	**Poor**	**No Control/ Not Tested**
Customer Inherent Risk Rating (IRR)	**Significant**	Medium	High	Significant	Significant
	High	Low	Medium	High	High
	Medium	Low	Low	Medium	Medium
	Low	Low	Low	Low	Low

6. Business Risk

What is business risk?

ML/TF business risk is the risk or vulnerability of a business operations customers to money laundering or terrorist financing activities. ML/TF business risk is significantly influenced by where the business operations are located, the use of third parties, and the ML/TF risks resulting from employees.

Business inherent risk

Business inherent risk is assessed through a combination of business operations risk and employee risk.

Business operations risk

Business operations risk is a combination of business location risk and business third party risk assessments:

- Business location risk assesses where business operations are located, based, or operate out of. Where business operations are in a higher ML/TF risk country it may contribute to rating the business operations as representing a higher ML/TF risk. The higher the percentage of business operations overseas and the higher the percentage in countries rated as high or restricted, the higher the business location risk rating.
- Business third party risk assesses the use by the business of third parties to undertake some or all the AML controls required by relevant AML law and regulation. Where a business uses third parties to operate AML controls but has inadequate governance and oversight of the activities of the third party, it may contribute to rating the business operations as representing a higher ML/TF risk.

Business third party risk is assessed as follows:

Rating	Outsourced Control Risk
High	The business does not know whether it uses third parties to operate AML controls. OR The business does use third parties to operate AML controls but does not know whether the outsourcing arrangements are fully documented or if the third party is regulated on the same/a similar basis. OR The business does use third parties to operate AML controls, but either the outsourcing arrangements are not fully documented, or the third party is not regulated on the same/similar basis.
Medium	The business uses third parties to operate AML controls, and the outsourcing arrangements are fully documented, and the third party is regulated on the same/similar basis.
Low	The business does not use third parties to operate AML controls.

Business operations risk is assessed using the following matrix:

Business Operations Risk		Outsource Control Risk			
		High	**Medium**	**Low**	**Unknown**
Business Location Risk	**High**	High	High	Medium	High
	Medium	High	Medium	Medium	High
	Low	Medium	Medium	Low	High
	Unknown	High	High	High	High

Additional contextual data

The following additional data that provides context to the risk of outsourcing AML controls to third parties is collected:

- The nature of the AML controls that are undertaken by third parties;
- The formal documentation of outsourcing arrangements; and
- The regulatory status of the third-party service provider performing AMLcontrols.

Employee risk

Employee risk is a combination of employee good-standing risk and employee role risk assessments:

- Employee good-standing risk assesses whether employees have been subject to criminal conviction and other adverse information. Employees subject to criminal conviction and other adverse information identified through screening, are considered to represent a higher ML/TF risk. The higher the percentage of employees with adverse screening results, the higher the employee good-standing risk rating.
- Employee role risk assesses the extent to which the organisation employs people in roles that are recognized as having increased vulnerability to being used to facilitate laundering money or finance terrorism. The higher the percentage of employees in higher risk roles, the higher the employee role risk rating.

Employee risk is assessed using the following matrix:

Employee Risk		Employee Role Risk			
		High	**Medium**	**Low**	**Unknown**
Employee Screening Risk	**High**	High	High	Medium	High
	Medium	High	Medium	Medium	High
	Low	Medium	Medium	Low	High
	Unknown	High	High	High	High

Additional contextual data

The details of additional controls applied to employees in higher risk roles are collected to provide context.

Inherent business ML/TF risk is assessed by applying a combination of business operations risk and employee risk, using the following matrix:

		Business Inherent Risk Rating (IRR)Employee Risk		
		High	**Medium**	**Low**
Business Operation Risk	**High**	Significant	High	Medium
	Medium	High	Medium	Medium
	Low	Medium	Medium	Low

Business residual risk

Residual business ML/TF risks are assessed by overlaying the inherent ML/TF risk with an assessment of the controls to mitigate those risks, using the following matrix:

Business Residual Risk Rating (RRR)		Control Assessment			
		Excellent	**Adequate**	**Poor**	**No Control Not Tested**
Business Inherent Risk Rating (IRR)	**Significant**	Medium	High	Significant	Significant
	High	Low	Medium	High	High
	Medium	Low	Low	Medium	Medium
	Low	Low	Low	Low	Low

7. Channel Risk

What is channel risk?

ML/TF risk is significantly influenced by the nature and/or attributes of the channels used to deliver products and services to customers.

Channel risk is determined by whether the delivery of a product or service involves face to face contact with the customer, as face to face contact limits the ability for customer anonymity and facilitates establishing whether the customer is who they are claiming to be.

The use of third parties as part of the delivery chain of a product or service also creates a higher ML/TF channel risk.

Channel inherent risk

Channel inherent risk is assessed through a combination of non-face to face customer engagement risk and third-party risk.

Non-face to face risk

Non-face to face risk assesses the extent to which customers are not met face to face. Where a customer is not met in person (face to face) there is an increased vulnerability that the customer may not be who they claim to be, which may contribute to rating the channels used by the organisation as representing a higher ML/TF risk. The higher the percentage of customers that are not met face to face, the higher the non-face to face risk rating.

Additional contextual data

The methods used to engage customers or deliver products and services to customers is collected to provide context to the risk of the channels used.

Third party risk

Third party risk is a combination of third-party use by the organisation to engage customers and third-party location risk assessments:

- Third party use risk assesses the use of third parties to engage and attach customers for their products and services. The level of use of third parties to engage customers may contribute to rating the channel as representing a higher ML/TF risk. The higher the percentage of customers engaged through third parties, the higher the third-party use risk rating.
- Third party location risk assesses where third parties used by the organisation to engage customers are located, based, or operate out of. Where third parties are in a higher ML/TF risk country it may contribute to rating the channels used by the organisation as representing a higher ML/TF risk. The higher the percentage of third parties overseas and the higher the percentage of third parties in countries rated as high or restricted, the higher the third-party location risk rating.

Third party risk is assessed using the following matrix:

Third Party Risk		Third Party Use Risk			
		High	**Medium**	**Low**	**Unknown**
Third Party Location Risk	**High**	High	High	Medium	High
	Medium	High	Medium	Medium	High
	Low	Medium	Medium	Low	High
	Unknown	High	High	High	High

Additional contextual data

The following additional data that provides context to the channel risk is collected:

- Details of third parties used to engage customers or that undertake business activities/operations that involve customer contact.

Inherent channel ML/TF risk is assessed by applying a combination of third-party risk and non-face to face risk, using the following matrix:

Channel Inherent Risk Rating (IRR)		Third Party Risk		
		High	**Medium**	**Low**
Face to Face risk	**High**	Significant	High	Medium
	Medium	High	Medium	Medium
	Low	Medium	Medium	Low
	Unknown	High	High	High

Channel residual risk

Residual channel ML/TF risks are assessed by overlaying the inherent ML/TF risk with an assessment of the controls to mitigate those risks, using the following matrix:

Channel Residual Risk Rating (RRR)		Control Assessment			
		Excellent	**Adequate**	**Poor**	**No Control/ Not Tested**
Channel Inherent Risk Rating (IRR)	**Significant**	Medium	High	Significant	Significant
	High	Low	Medium	High	High
	Medium	Low	Low	Medium	Medium
	Low	Low	Low	Low	Low

8. Product / Service Risk

What is product / service risk?

ML/TF risk is significantly influenced by the nature and/or attributes of products and services.

Product / service risk is determined by whether the attributes of a product or service offer features or characteristics that can be used to facilitate money laundering and/or terrorist financing.

The methodology applied to assess product ML/TF risk is based on different attributes that are risk factors to whether the product or service is more vulnerable and therefore is higher risk from a money laundering and financing terrorism perspective.

Product inherent risk

Inherent product or service ML/TF risk is assessed by applying a combination of a flexibility rating and higher risk product classification.

Product/Service flexibility

The flexibility of a product or service is an assessment of how much functionality and capability it allows the customer.

The risk factors that make a product or service more vulnerable to ML/TF risk are:

- Customer or user anonymity;
- The use or access by third parties;
- The availability or use overseas; and
- The ability to use or gain access to cash.

Product / Service flexibility is assessed through a series of 20 Yes / No questions that identify the features and characteristics that may make the product/service vulnerable, and each product is rated as follows:

Rating	Product / Service Flexibility Risk Factor
Low	A yes score of **0 to 5** means the product/service is not flexible and is therefore not very vulnerable to ML/TF risk. The dynamics of the product are not attractive to money launderers and terrorist financiers.
Medium	A yes score of **6 to 8** means the product/service is somewhat flexible and is therefore vulnerable to ML/TF risk. The dynamics of the product/service are moderately attractive to money launderers and terrorist financiers.
High	A yes score **9 or over** means the product/service is very flexible and is therefore highly vulnerable to ML/TF risk. The dynamics of the product/service are highly attractive to money launderers and terrorist financiers.

Higher risk products and services

Products or services that have been identified as representing a higher ML/TF risk by typologies or case studies, are considered to represent a higher risk.

Where the product or service has been determined to be higher risk, a risk flag is assigned, which increases the inherent risk rating derived from product/service flexibility rating.

For example, if a yes score of 0 to 5 in the product flexibility risk factors would result in a medium risk rating, not low. A medium would become high, and high would become significant.

Additional contextual data

The following additional data that provides context to the risk of the product or service is collected:

- The percentage of customers using the product or services;
- The amount of revenue the product or service generates;
- Whether the product or service is subject to monitoring; and
- The number of reports of suspicion made in the last 12 months involving the product or service.

Inherent product or service ML/TF risk is assessed by applying a combination of flexibility rating and higher risk product classification, using the following matrix:

Product Inherent Risk Rating (IRR)		**Higher Risk Product / Service**	
		Yes	**No**
Product Service Flexibility	**High**	Significant	High
	Medium	High	Medium
	Low	Medium	Low

Product / Service residual risk

Residual product / service ML/TF risks are assessed by overlaying the inherent ML/TF risk with an assessment of the controls to mitigate those risks, using the following matrix:

Product / Service Residual Risk Rating (RRR)		**Control Assessment**			
		Excellent	**Adequate**	**Poor**	**No Control Not Tested**
Product / Service Inherent Risk Rating (IRR)	**Significant**	Medium	High	Significant	Significant
	High	Low	Medium	High	High
	Medium	Low	Low	Medium	Medium
	Low	Low	Low	Low	Low

9. Country Risk

What is country ML/TF risk?

Country risk is the assessment of a country's or jurisdiction's vulnerability to money laundering, terrorism financing, and targeted financial sanctions. Country risk ratings are relevant to the location of business operations, customers and third party distributors.

Country risk factors

The following sources are used to identify the various risk factors applied as part of the country risk assessment:

Risk Factor	Source
Targeted Financial Sanctions	United Nations European Union United States of America Other Countries - Australia - New Zealand - United Kingdom - Canada - Singapore - Hong Kong - South Africa - Brunei - Ireland
AML Concerns	FATF High-risk and Other Monitored Jurisdictions
Terrorism Vulnerability	US Department of State's Country Report on Terrorism
Illicit Drug Vulnerability	US International Narcotics Strategy Control Report
Corruption Vulnerability	Transparency International Corruption Perceptions Index
Money Laundering Vulnerability	US International Narcotics Strategy Control Report
Financial Secrecy	Financial Secrecy Index
Kimberley Process	Kimberley Process Participant List
FAFT Membership	FATF Members and Observers

Country risk assessment methodology

The following criteria is used to apply each country with their risk ratings.

Ratings	Criteria
Restricted	Any country with people or entities currently subject to targeted financial sanctions imposed by the United Nations, US (OFAC), EU or Other Countries listed in 'Country risk factors' section above. Targeted financial sanctions include: - Freezing of assets, financial measures, restrictions on investments, or arms export involving financial assistance (EU) - Blocking of property, financial restrictions (US)
High	Any country that is currently subject to any other sanctions imposed by the UN, US, EU such as specific trade embargo's; or Any country that has been expelled or resigned from the Kimberley process (if not also financially sanctioned / restricted); or Any country that has historically been sanctioned by UN, US, EU, or Other Countries listed in 'Country risk factors' section above but those sanctions have been lifted; or Any country that is **not** a FATF member and appears on **2** or more of the following lists, OR any country that **is** a FATF member and appears on **3 or more** of the following lists: i) Listed by the FATF as having strategic AML/CFT deficiencies ii) Listed by the US State Department as being a State Sponsor of Terrorism or Terrorist Safe Haven iii) Listed on the US International Narcotics Strategy Control Report as a Major Money Laundering Concern iv) Listed on the US International Narcotics Strategy Control Report as a Major Illicit Drug Producing Country or Drug Transit Country v) Listed on the Transparency International Corruption Perceptions Index with a score of 40 or less vi) Listed on the Financial Secrecy Index, issued by the Tax Justice Network, with a score of 60 or more

Ratings	Criteria
Medium	Any country that is **not** a FATF member and appears on only **1** of the following lists. OR any country that **is** a FATF member and appears on **2** of the following lists: i) Listed by the FATF as having strategic AML/CFT deficiencies ii) Listed by the US State Department as being a State Sponsor of Terrorism or Terrorist Safe Haven iii) Listed on the US International Narcotics Strategy Control Report as a Major Money Laundering Concern iv) Listed on the US International Narcotics Strategy Control Report as a Major Illicit Drug Producing Country or Drug Transit Country v) Listed on the Transparency International Corruption Perceptions Index with a score of 40 or less Listed on the Financial Secrecy Index, issued by the Tax Justice Network, with a score of 60 or more
Low	Any country that does **not** appear on **any** of the following lists, OR any country that **is** a FATF member but only appears on **1** of the following lists: i) Listed by the FATF as having strategic AML/CFT deficiencies ii) Listed by the US State Department as being a State Sponsor of Terrorism or Terrorist Safe Haven iii) Listed on the US International Narcotics Strategy Control Report as a Major Money Laundering Concern iv) Listed on the US International Narcotics Strategy Control Report as a Major Illicit Drug Producing Country or Drug Transit Country v) Listed on the Transparency International Corruption Perceptions Index with a score of 40 or less Listed on the Financial Secrecy Index, issued by the Tax Justice Network, with a score of 60 or more