TATA BLUESCOPE STEEL

Tata BlueScope Steel Pvt Ltd (TBSPL)

Anti-Money Laundering (AML) Policy

Ver 1.0

Ethics Office
July 01, 2022

Table of Contents

1. Glossary

Sr. No.	Abbreviation	Particulars
1.	AML	Anti-Money Laundering
2.	AMLCO	AML Compliance Officer
3.	EC	Ethics Counsellor
4.	CTF	Counter Terrorist Financing
5.	EDD	Enhanced Due Diligence
6.	KYC	Know Your Customer
7.	MD	Managing Director
8.	ML	Money Laundering
9.	PMLA	Prevention of Money Laundering Act
10.	TF	Terrorist Financing
11.	TBML	Trade Based Money Laundering

2. Policy Statement

Tata BlueScope Steel Pvt. Ltd. (referred as "TBSPL" or "the Company" henceforth) dedicates itself to its Code of Conduct. In conducting business with due skill, care and diligence, the Company seeks always to comply with relevant laws, rules, regulation, codes and standards of good practice.

Clause # 2 of the Company's Code of Conduct states that "We shall comply with all applicable anti-money laundering, anti-fraud and anti-corruption laws and we shall establish processes to check for and prevent any breaches of such laws."

As a next step towards this, TBSPL has introduced its Anti Money Laundering (AML) Policy herewith. We are committed to acting professionally, fairly and with integrity in its business dealings and relationships wherever it operates and that we must conduct business only with reputable customers who are involved in legitimate business activities and whose funds are derived from legitimate sources.

The fight against money laundering & terrorist financing is a priority for the Company. We recognize that this fight is a team effort and ensure that its policies, procedures, systems and controls appropriately and adequately address the requirements of Know your Customer (KYC), Anti Money Laundering (AML)/Counter Terrorist Financing (CTF) Law and regulations.

Refer **Annexure 1** for guidance on Money Laundering (ML), Terrorist Financing (TF) and Trade Based Money Laundering (TBML)

We also support and adhere to the major international organizations, which collectively set and enforce standards for anti-money laundering & combating terrorist financing policies and programmes such as FATF (Financial Action Task Force), United Nation (UN), The European Union (EU), The Organization of American States - The Office of Foreign Assets Control (OFAC) and the local regulatory authorities.

In conducting business with due skill, care and diligence, the Company seeks always to comply with relevant laws, rules, regulation, codes and standards of good practice.

We are continuously updating our processes, systems and technology and training our staff, to assure that we are well equipped to combat money laundering, terrorist financing and other financial crimes to the extent feasible. We are fully committed to remaining constantly vigilant to prevent the use of our products and services by those who would misuse them.

As our responsibility, we carry out periodic assessment of the adequacy and effectiveness of our KYC, AML / CTF policies, procedures and systems in preventing money laundering / terrorist financing. A similar assessment will be done periodically/ as and when required. In the case of any changes required, notification will be sent to Board and post its approval the same will be implemented in the organisation.

The policy should be read in conjunction with:

- Code of Conduct
- Whistle-Blower Policy
- The Anti-Bribery Anti-Corruption policy
- Any other relevant policies as implemented from time to time.

3. Purpose of the Policy

The purpose of the Company's AML policy is to prevent its involvement in any money laundering activity whether by deemed conversion of illegally gained money or whether directly or indirectly, even where such involvement may be unintentional.

- To ensure that TBSPL is compliant with various legislative/ regulatory provisions related to AML/ KYC
- To protect the Company from being exploited as a channel for money laundering and terrorist financing.
- To protect and enhance the reputation of the Company.

Towards this objective, TBSPL must conduct business only with reputable customers, distributors, business partners, service providers, contractors and consultants who are involved in legitimate business activities and whose funds are derived from legitimate sources.

4. Scope & Applicability of the policy

This policy is applicable to all individuals working at all levels and grades, including directors, senior managers, officers, trainees, interns, other employees (whether permanent, fixed-term or temporary), consultants, contractors, seconded staff, casual workers and agency staff, agents, or any other person associated with the Company and other such persons including those designated by the Company AML Compliance Officer/Ethics Counsellor from time to time (all of the aforesaid being collectively referred to as "TBSPL Personnel").

5. Definitions

a) *Anti – Money Laundering*

Anti-money laundering (AML) is a set of procedures & controls implemented to detect and prevent money laundering activities. Prevention of money laundering encompasses following aspects:

- Know Your Customers / Distributors/ Business Associates / Employees (KYC) - Identifying/ verifying the identity of customers, distributors, business associates as well as employees to be associated with the Company through prudent due diligence at the point of on-boarding/ empanelment and on-going maintenance of relationship.

- Customer/ Distributors/ Business Partner / Employees Due Diligence - Due diligence refers to various checks performed to effectively assess the identity of business partners and potential risks they may pose from a money laundering/ terrorist financing perspective. Due diligence is carried out by collecting information/ documents to identify and establish purpose, nature of business relationship and ownership. The nature and extent of due diligence will depend on the risk perceived and local regulatory requirements.

- Transaction monitoring - Ongoing monitoring of transactions to detect and control potential money laundering

activities.

- Reporting suspicious activities -Periodically reporting any unusual activities from AML/CTF standpoint to regulatory authorities and in line with the reporting procedures

b) Business Associates

A 'Business Associates' is defined as a person/entity who is engaged in a financial transaction or activity with the Company and includes a person on whose behalf the person who is engaged in the transaction acts. In context of this policy, it also includes customers, distributors, external processing agencies, vendors and suppliers etc.

c) Beneficial owner

A Beneficial owner means the natural person who ultimately owns or controls a client/ business partner and or, the person on whose behalf a transaction is being conducted and includes a person who exercises ultimate effective control over a juridical person.

d) Controlling parties

Controlling parties are individuals or entities with direct or indirect control over the relationship/ account created with the Company. For KYC purposes, controlling parties are defined as authorized signatories, power of attorney holders, executive management of the organisation (e.g. partners, directors etc.). Different relationship/account types and transactions could involve different controlling parties depending on who is interacting with them.

e) Politically exposed person (PEP)

As per Financial Action Task Force (FATF) politically exposed person (PEP) is defined as an individual who is or has been entrusted with a prominent public function. Due to their position and influence, it is recognised that many PEPs are in positions that potentially can be abused for the purpose of committing money laundering and related predicate offences, including corruption and bribery, as well as conducting activity related to terrorist financing.

This also includes an immediate family member, or known close associate of such person.

For example, Heads of State or of Government, senior politicians, judicial or military officials, senior executives of state-owned corporations etc.

f) Shell company

Shell company is a company which has no physical presence, business and assets. These companies are just used as a financial vehicle to move funds.

Shell companies can be identified through public domain information, media reports, screening and regulator's orders.

g) Sanction countries/ entities/ individuals

- Countries - Sanctions are imposed on a country that does not apply sufficient legislations in terms of combating money laundering and terrorist financing or which is known to be affected by criminal activities and terrorism. The list of sanctioned countries is available on the website of Office of Foreign Assets Control (OFAC) https://sanctionssearch.ofac.treas.gov/
- Entities / individuals - Any entity/individuals who are associated with terrorism/money laundering are included

in the Sanctions list. The list is maintained by United Nations Security Council and published on their website https://scsanctions.un.org/search/.

h) Tip-Off

Tipping off is a situation where, intentionally/unintentionally, confidential information` related to investigation is disclosed to the suspect individual/entity. For example: Internal investigation details shared by employee with the customer/ distributors/ business partner.

i) Dual use goods

Dual use goods are items which can be used for both civil and military purpose e.g. software, technology, document, diagrams etc. These goods can also include raw material & components such as bearing, aluminium alloys or laser etc.

6. Roles and Responsibilities

a) Board of directors

Board of directors of the Company are responsible for ensuring that an effective KYC, AML and CTF programme is put in place by establishing procedures and defining adequate guidelines for its effective implementation and ensuring appointment of an AML Compliance Officer.

b) AML Compliance Officer (AMLCO) and Ethics Counsellor (EC)

The Company shall, from time to time, designate an employee of sufficient seniority, competence and independence as the compliance officer to ensure compliance with the provisions of this AML policy. The **Chief Financial Officer** has been designated as the Compliance Officer for overseeing and monitoring the AML policy.

All reports, complaints, doubts or concerns in relation to this AML policy shall be raised to the AMLCO/ EC who shall also be responsible for investigating any suspected violation of the AML Policy.

AMLCO has the following responsibilities

- Support the board of directors in managing the money laundering /terrorist financing risk.
- Report suspicious transactions to regulatory authorities.
- Ensure prompt response to information requested by regulators in relation to AML/ CTF issues.
- Monitor effectiveness of the AML/CTF training programmes.

EC has the following responsibilities

- Ensure that appropriate procedures and systems are established to enable compliance with the policy.
- Periodically update AML policies in line with guidelines in changing business and regulatory environment.

c) Staff Members

- All the staff members are responsible to safeguard the Company from being used by external entities for money laundering or any other illegal purposes.
- Staff interacting with customers/distributors/business partners or handing transactions are the first line of defence for the company. The awareness of AML policy and related training will be essential for them.

- It is staff's responsibility to keep themselves updated with policies and procedures related to their role in the company. Staff also has an obligation of reporting suspicious activities to AMLCO/ EC.

7. Compliance Steps

Prevention of money laundering encompasses following aspects:

7.1 ***Know Your Customers*** / Distributors/ Business Associates / Employees (KYC) - Where appropriate, employees should conduct due diligence exercises and be familiar with the parties they are dealing with, at the point of on-boarding/ empanelment and on-going maintenance of relationship. Due diligence refers to various checks performed to effectively assess the identity of business partners and potential risks they may pose from a ML/ TF perspective.

7.2 ***Transaction monitoring*** – TBSPL Personnel are required to observe and record payments and transactions to ensure they are consistent with all established policies and procedures and follow global financial standards for acceptable forms of payment. Such ongoing monitoring of transactions is essential to detect and control potential money laundering activities. Special caution should be exercised in context to the following red flags (Refer Annexure 1 part e) which may purport to potential money laundering.

7.3 ***Keeping records***: Employees should always keep current, complete and accurate records of every business transaction.

7.4 ***Reporting suspicious activities*** -Periodically reporting any unusual activities from AML/CTF standpoint to regulatory authorities and in line with the reporting procedures. Suspicious transactions are identified during:

- Interaction with customer/ distributors/ business partners during purchase/sale.
- Verification of documents.
- Ongoing transaction monitoring.

A Suspicious transaction is one where the nature of transaction:

- Gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime specified in the schedule to the PMLA, regardless of the value involved.
- Appears to be made in unusual circumstances or, is of unjustified complexity and appears to have no economic rationale.
- gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism or other forms of criminal activity

7.5 ***Reporting/action by the AMLCO***: Any suspicious activity identified must be reported to AMLCO/EC. The AMLCO is required to record the reason for treating the transaction as suspicious or non-suspicious post investigation.

AMLCO will report the suspicious transaction to the regulatory authority. The Company must ensure there is no tipping-off at any level.

Based on the facts and circumstances of an incident covered in a Report, the AMLCO shall take one or more steps, such as (a) probe into the incident themselves, (b) set up an internal enquiry into the incident, (c) in case of Aggravated Cases determine and recommend whether a reporting of the incident should be made to the appropriate authority. (Aggravated Cases shall mean incidents that need to be reported to relevant regulatory or enforcement authorities. All Aggravated Cases must be escalated, without delay, by the MD to the Board).

7.6 ***Cooperate fully for enforcing AML laws***: The AMLCO shall be the Company's point of contact for coordinating with all law enforcement and regulatory agencies for all compliance reporting and investigations. Employees shall render full support to the AMLCO as well as cooperate fully with any internal investigation team set up by the AMLCO or the MD or the Board, or with any external investigation.

8. Consequences of violation of this AML policy

In case of violations of the AML Policy, the AMLCO shall, after considering inputs, if any, from the MD, have the discretion to do the following:

a) Corrective Action: If necessary, corrective actions shall be prescribed by the AMLCO to appropriate managers, officers, or other employees for implementation.

b) Penalties: The AMLCO shall, based on the investigation reports (if any) have the discretion to recommend appropriate disciplinary action, including suspension and termination of service, against such a defaulting person. Final decision rests with the MD.

Depending on the nature and scale of default of the AML Policy by the defaulting person, the AMLCO and MD may also recommend to the Board to commence civil and/or criminal proceedings against such an employee in order to enforce remedies available to our Company under applicable laws.

9. Customer/ Distributors/ Business Associates Acceptance Policy

The objective is to enable the Company to identify customers/ business partners with whom Company will not establish any relationship. The relationship will not be accepted under the following circumstances:

- With any anonymous or fictitious entity
- When the Company is unable to apply appropriate customer due diligence measures,
  i.e. unable to verify the identity and /or obtain required documents either due to non- cooperation of the customer or non-reliability of the documents/information furnished by the customer.
- With any sanctioned individual/ entity/country as detailed in section 6.9.
- In any manner with any person, if it is known that the Person/ entity is
  - Barred by the law of the land
  - Belongs to or affiliated to Terrorists and Terrorist & Banned Organisations. List of such organisations / entities is available on the website of Office of Foreign Assets Control (OFAC) i.e., https://sanctionssearch.ofac.treas.gov/
  - A shell company

10. Customer Identification, Know Your Customer (KYC) Policy

Customer identification means conducting client due diligence measures before establishing client relationship including identification and verification of the customer and the beneficial owner on the basis of documents to the extent feasible. The Company should collect sufficient information to establish the identity and genuineness of the customer/ distributors to the extent applicable.

Following general procedures are to be followed

- Verify customer identification evidence confirming the identity of the customer to ensure that customer is involved in legitimate business activities
- Discussions to understand their capabilities and credentials
- Site visits on a need basis
- Understand the ownership and control structure of the customer.
- Determine the natural person(s) who ultimately owns or controls the customer.
- In case the beneficial owner is a PEP, enhanced due diligence should be carried out.

List of acceptable identification documents are set out in the Annexure 2.

11. Identification of Beneficial Owner

The Company must aim to determine whether the customer/ distributor is acting on behalf of another person. In such case, officers/ employees may consider to obtain sufficient identification data to verify the identity of that other person to the extent feasible.

For customers that are legal persons or legal arrangements, officers/ employees of the Company must attempt to take steps to (to the extent possible):

- Understand the ownership and control structure of the customer.
- Determine the natural person(s) who ultimately owns or controls the customer.
- In case the beneficial owner is a PEP, enhanced due diligence should be carried out.

12. Risk Based Approach (RBA)

RBA means to identify and assess the money laundering and terrorist financing risks in accordance with the level of risk posed by the customer / distributors/ business associates.

RBA allows the Company to effectively use their resources and apply enhance measures in the event higher risk is identified. RBA assists in identifying the level of due diligence required for customers/ distributors/ business partners.

Company must attempt to adopt RBA to address management and mitigation of various ML/TF risks. In order to adopt RBA the Company has developed below categories of customers/ distributors/ business partners:

a) Prohibited

All the customers/ distributors/ business partners listed below are classified under prohibited category:

- Barred by the law of the land.
- Belongs to or affiliated to Terrorists and Terrorist & Banned Organisations. List of such organisations / entities is available on the website of Office of Foreign Assets Control (OFAC) i.e. https://sanctionssearch.ofac.treas.gov/
- A shell company.

b) High Risk

Company must attempt to consider below indicative list of customers in high risk category:

- Politically Exposed Persons (PEPs).
- Customer associated with high risk countries/ tax haven countries (Annexure 2).
- Distributor/ dealer dealing with high value cash.
- Non-profit organisations/ Charitable trust etc.
- Customers involved in instances of third party payments.
- Any other customer, company find appropriate.

c) Low Risk

All the other customers who do not fall under Prohibited and High Risk customer should be classified under Low risk.

13. Due Diligence and Record Keeping

There are different levels of due diligence applied to customer based on risk assessment.

a) Simplified Due Diligence (SDD)

Simplified due diligence is applied to all the customers for which minimal potential money laundering and terrorist financing risk exists.

b) Enhanced Due Diligence (EDD)

EDD refers to additional information collection and conducting advanced background checks on individual/entities. In case there is a perception of high risk of ML/TF, the Company must aim to conduct EDD to gain deeper understanding of customer/ distributors/ business partner's activities. As a part of EDD company must attempt to collect documents/information of the customers to the extent feasible.

- Adverse information/ media checks/ public domain search.
- Credit reports such as D&B report etc. to the extent feasible (wherever necessary).
- Physical meetings with Customer or Site visits (case to case basis) or business associates references.

c) De-empanelment / Blacklisting of Customers/ Distributors/ Business Associates

The Company must aim to consider blacklisting the customers/ distributors/ business associates in case they are associated with money laundering/ terrorist financing. Once the customer/ distributors/ business partners are blacklisted, no services/products will be offered/obtained to them in future. The data base of blacklist should be updated and used while on-boarding new customers/ distributors/ business partners to the extent applicable.

14. On-going Due Diligence / Evaluation and Record maintenance

The Company shall aim to perform on-going periodic due diligence (PEP review/Sanctions screening) on their customer, distributor and business associates to mitigate ML/TF risks. The Company considers maintaining all documents and records related to the following for **five years** in line with PMLA requirements - KYC and due diligence documents, Transaction records, Trainings records etc.

15. Employee Training and Awareness

The Company attempts to implement ongoing employee training programme so that all the staff members are adequately trained in AML/CTF guidelines. While considering the training needs, the Company looks into the existing experience, skill and abilities, functions and role intended, outcome of earlier training etc. Company carries out review of training needs at regular intervals in order to ensure that the objectives of the trainings are met depending on role of the staff members.

16. Periodic review & assessment of compliance with AML guidelines

The Company shall consider periodic review and assessment of AML compliance programme to align with internal/ regulatory development (if any).

Anoop Kumar Trivedi
Managing Director

Annexure 1 – Guidance on Money Laundering (ML), Terrorist Financing (TF) and Trade Based Money Laundering (TBML)

Money laundering is a global problem, and many countries, and organizations have enacted laws to combat it. Compliance with AML and anti-terrorism laws and regulations requires an awareness of possible 'Red Flags' or suspicious activities, which may arise in the course of conducting business. When 'Red Flags' are identified, an appropriate level of additional due diligence must be performed and additional approvals should be obtained.

a) Prevention of Money Laundering Act, 2002:

The Government of India has enacted the Prevention of Money Laundering Act, 2002 and issued rules and regulations thereunder ("PMLA") for preventing money laundering and countering the financing of terrorism in India, with effect from July 1, 2005. The PMLA defines the offence of money laundering as "Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime and projecting it as untainted property shall be guilty of offence of money laundering."

The term 'proceeds of crime' has been defined under Section 2(u) of the PMLA as "any property derived or obtained, directly or indirectly, by any person as a result of criminal activity relating to a scheduled offence or the value of any such property." The definition of 'proceeds of crime' also implies that assets can be tainted by conversion. Therefore, if the 'proceeds of crime' are utilized to purchase another asset, by conversion, that asset could also be considered to be a 'proceed of crime' replacing the tainted money. Under the provisions of the PMLA, proceeds of crime can be attached in the possession of any person, whether or not such person was involved in the offence of money laundering.

b) Money Laundering

Money Laundering is the process whereby criminals attempt to hide and disguise the true origin and ownership of the proceeds of their criminal activities thereby avoiding prosecution, conviction and confiscation of the criminal funds. The source of the proceeds may include drug trafficking, terrorism, organized crime, illicit trade, fraud and other related crimes.

There are three stages of money laundering which are explained as under:

i. Placement

Involves introduction of illegally obtained fund into the financial system, usually through financial institutions. This can be achieved through purchase of goods in cash etc.

ii. Layering

Usually consists of a series of transactions, through conversion and movement of funds, designed to conceal the origin of funds. This may be accomplished by creating layers of transactions by moving the illicit funds between accounts, between businesses, and by buying and selling goods from/to various parties/countries until the original source of the money is virtually untraceable.

iii. Integration

This stage involves re-entering funds into legitimate economy. Once the illegitimate money is successfully integrated into the financial system, these illicit funds are reintroduced into the economy and financial system and often used to purchase legitimate assets, fund legitimate businesses, or conduct other criminal activity. The transactions are made in such a manner so as to appear as being made out of legitimate funds.

c) *Terrorist Financing (TF)*

TF is the process by which terrorists fund their operations in order to perform terrorist acts. Terrorist financing relates to provision or collection of funds to carry out an act of killing or seriously injuring a civilian with the objective of intimidating a section of people or compelling a government to do or to abstain from doing any act.

d) Trade based money laundering (TBML)

As per FATF, trade-based money laundering is defined as the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimise their illicit origins.

There are various common techniques used by criminals to launder money, some of which are listed below:

- Under-invoicing - Exporting the goods with invoicing lower amount than market standard which helps importer to sell the goods in the market and generate thefunds.
- Over-invoicing - Exporting the goods with invoicing higher amount through which importer transfer the funds to exporter more than correct value.
- Multiple Invoicing - Creating more than one invoice for the same consignment exported to justify the reason of multiple payments. Multiple payments can be generated from various financial institutions.
- Over & under Shipment - Displaying over/ under shipment exported for receiving unreal credits in the account through trade transactions.
- False description of goods - Method of incorrect description of goods can be used to launder the money. E.g., exporter misrepresenting the quality or type of the goods on the invoice and customs documents.

e) Potential Red Flags

While an exhaustive list cannot be provided, set out below are indicative actions or situations or parties that - when appearing together or individually - should raise 'Red flag':

- Customers/ distributor/ business associates reluctant to provide complete information and/or provide insufficient, false, or suspicious information.
- The KYC documents appear as suspicious i.e. customer/ distributor submits false documents that appears to be alerted/ inaccurate etc.
- Customers/ distributor/ business associates unwilling to comply with the Company's KYC norms customers / distributor/ business associates who appear to be acting as an agent for another company or individual, but decline or are reluctant to provide information regarding the company or individual.
- Refusal to identify owners or controlling interests.
- Beneficial owner of the customer/ distributor is located at sanctioned, high risk, and tax heaven countries.
- The transaction has no apparent or visible economic or lawful purpose.
- Customers or suppliers who express concern about, or want to avoid, reporting or recordkeeping requirements.
- Customer transactions are more than expected level of activities.
- The purchase of products, or a larger volume purchase, that appears to be inconsistent with a customer's normal ordering pattern, and in the absence of any legitimate business reason such as a special price promotion
- Selling or buying products within same jurisdiction having an intermediary located abroad / unnecessary involvement of third parties.

- Frequent changes in bank accounts by customer/ distributors.
- Customers/ distributors whose address is not a physical site/ who do not have a physical presence.
- Insistence on making cash or cash equivalent payments. Acceptance of such amounts of cash or cash equivalents as a form of payment by our Company is strongly discouraged. Cash payments are commonly used by money launderers and leave very little in the way of audit trails. Alternative methods of payment which provide a stronger audit trail should be offered. Particular care should be taken with regard to customers and suppliers who structure these payments to avoid the relevant government reporting requirements for cash and cash equivalent payments (for example by making multiple smaller payments or payments from multiple sources)
- Multiple partial payments from various parties on behalf of a single customer and/or multiple partial payments from various locations. Also included are "double endorsed" or "third party" cheques, where a customer endorses over to a company as payment for their invoice a cheque that was originally made out to the customer.
- Customers making a funds deposit followed by an immediate request that the money be wired out or transferred to a third party, or to another firm, without any apparent business purpose.
- Any other transaction of unusual or inconsistent in nature.

Annexure 2 – List of acceptable KYC documents

Customer/Client	Acceptable Documents
Private Limited Companies	a. Certificate of incorporation b. Memorandum and Articles of Association c. A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf d. An officially valid document in respect of managers, officers or employees holding an attorney to transact on its behalf.
Partnership firms	a. Registration certificate b. Partnership deed c. An officially valid document in respect of the person holding an attorney to transact on its behalf
Trusts	a. Registration certificate b. Trust deed c. An officially valid document in respect of the person holding a power of attorney to transact on its behalf
Proprietorship Concerns	a. Registration certificate (in the case of a registered concern) b. Certificate/licence issued by the Municipal authorities under Shop & Establishment Act c. Sales and income tax returns d. CST/VAT certificate/ GST certificate (provisional/final). e. Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities

Annexure 3 - List sanctioned & high-risk countries

Indicative List of Sanctioned countries:

Country Name	Categorisation
North Korea	Sanctioned
Syria	
Iran	
Cuba	
Ivory Coast	

Indicative List of High, medium, low risk countries

Country Name	Categorisation
Afghanistan	High Risk
Nigeria	
Tajikistan	
Laos	
Ghana	
Zimbabwe	
Uganda	
Cambodia	
Tanzania	
Kenya	
Liberia	
Myanmar	
Zambia	
Namibia	
Lebanon	
Yemen	
Turkey	
Pakistan	
Kuwait	Medium Risk
China	
Saudi Arabia	
Georgia	
Peru	
South Africa	
Luxembourg	
Egypt	
Bahrain	
Mexico	
Finland	Low Risk
New Zealand	
Denmark	
Sweden	
Malta	
Poland	

Notes - For any other country listed above, staff member may approach to AMLCO/ EC. The above indicative list is based on FATF, AML Basel Index information etc.