Application of a Risk-Based Approach

CAMILLERI PREZIOSI
ADVOCATES

30th November 2021

Peter Mizzi

www.21Academy.education

Agenda

- Explaining the Risk-Based Approach;
- Risk Assessment;
- Business Risk Assessment;
- Business Risk assessment process;
- Customer Risk Assessment;
- Jurisdictional Risk Assessment;
- De-risking vs financial inclusion

CAMILLERI PREZIOSI
ADVOCATES

What is a Risk-Based Approach?

A risk based approach is **a process that allows you to identify potential high risks of money laundering and terrorist financing and develop strategies to mitigate them.** Once your compliance program reduces those highest risks to acceptable levels, you move on to lower risks.

Risk-based approaches to AML are important **because they take a more proactive stance when it comes to illicit activity**. Rather than waiting until illegal transactions and transfers have already taken place, an RBA allows you to implement stop gaps

Benefits of a risk-based approach

- Allows management to differentiate between the firm's customers in a way that matches the risk in the particular business
- Allows SM to apply its own approach to the firm's procedures, systems and controls in particular circumstances
- Helps to produces a more cost-effective system; and
- Ensures that attention and resources can be concentrated where there is the greatest risk.

Risk assessment

Every subject person shall take appropriate steps, proportionate to its nature and size, to identify and assess the risks of ML/FT that arise out of its activities or services, taking into account risk factors including those related to customers, countries or geographical areas, products, services, transactions and delivery channels and shall furthermore take into consideration any national or supranational risk assessments relating to risks of ML/FT …

… the risk assessment shall be properly documented, and shall be made available to the FIAU and any relevant supervisory authority upon demand …

… the risk assessment shall be regularly reviewed and kept up-to-date

PMLFTR, Regulation 5

Levels of risk assessment

Supranational risk assessment (SNRA)

- To be undertaken by the EU Commission
- At least cover: (i) highest areas of risk to the internal market; (ii) the risks characterising relevant sectors; and (iii) the most widespread means used by criminals to launder their illicit activities
- Make recommendations to MS to address those risks on a 'comply or explain' basis
- Published within 2 years after adoption and updated biennially

National risk assessment (NRA)

- To be led by the National Co-ordinating Committee
- Covers domestic risks of ML/TF as well as international risks to Malta from money flowing into and out of the economy
- Help FIAU to identify areas where and what EDD measures should be applied

Entity-level risk assessment (RA)

- To be undertaken by the subject person
- Covers ML/TF risks specific to the subject person as well as other broader ML/TF risks which may increase its ML/TF risk exposure

SNRA 2019 outcomes

Sector	Main risks
Cash and cash-like assets	• Diamonds, cars, watches, and other similar items which are not closely supervised
Financial sector	• Unscrupulous behaviour of agents and distributors, • Fintech developments allowing anonymity and speed of transactions • Virtual currency providers – no level playing field in regulation; still a nascent area
Non-financial sector	• Real estate agents, lawyers, accountants and tax advisors are all prone to being misused for ML/FT purposes
Gambling sector	• Online gaming in particular is seen to present a high risk of ML/FT due to the very large number of transaction flows and the lack of face-to-face interaction • Land-based betting and poker also poses a high risk due to ineffective controls
NPOs	• Used to hide beneficial ownership • Not supervised closely from an ML/FT perspective
New products / services	• Professional football • Free ports • Investor citizenship and residence schemes

NRA 2018 outcomes

Summary of Malta's ML threat assessment
Domestic proceeds of crime

Overall level:	National ML threat	High

Domestic proceeds of crime	Medium-High
Foreign proceeds of crime	High

Sub-category	Threat level
Tax evasion	High
Local criminal groups	High
Drug trafficking	Medium-High
Fraud and misappropriation	Medium-High
Corruption and bribery	Medium-High
Smuggling	Medium
Theft and receipt of stolen goods	Medium
Armed robbery	Low
Living of the earnings of prostitution	Low
Usury	Low
Illegal gambling and violations of the Gaming Act	Low
Human trafficking	Low
Arms trafficking	Low
Smuggling of persons	Low
Unlicensed financial services	Low

Perspectives

- Malta's domestic ML threat is mostly driven by **tax evasion**, **local criminal groups**, **drug trafficking** and **fraud**
- **Tax evasion:** estimated to be about 5% of GDP (vs. an OECD average of approximately 3%)[1]
- **Local criminal groups:** revenues from the illicit market in Malta is estimated to be 1.4% of GDP vs. 0.9% EU average[2]
- **Drug trafficking:** The Police investigated drug trafficking and brought charges 254 times in 2012 – this crime is becoming a major generator of proceeds in Malta
- **Fraud** is the most prevalent suspected predicate offence

NRA 2018 outcomes (cont.)

Summary of Malta's ML threat assessment

Foreign proceeds of crime

Overall level:	National ML threat	High

Domestic proceeds of crime	Medium-High
Foreign proceeds of crime	High

Countries	Threat level	Perspectives
ML of foreign proceeds of crime threat level was calculated for a number of countries	High	• ML threat to Malta is **high** and driven **primarily by the threat of foreign proceeds of crime** • Malta's **large financial sector** is one of the biggest drivers of Malta's high threat from the laundering of foreign proceeds of crime • **Funds generated from offences committed in high-risk nearby countries** pose a high ML threat to Malta

NRA 2018 outcomes (cont.)

Summary of Malta's ML sectoral vulnerability assessment
Residual vulnerability

Sector	Residual	Sub-sectors	Sub-sector vulnerability		
			Inherent	Controls	Residual
Banking	Medium-High	Core domestic banks	High	Medium-low	Medium-High
		Non-core domestic & international banks	High	Medium-low	Medium-High
Securities	Medium-High	Collective investment schemes	Medium-High	Low	Medium-High
		Custodians	Medium-High	Low	Medium-High
		Foreign exchange	Medium-High	Low	Medium-High
		Fund administrators	Medium-High	Low	Medium-High
		Fund managers	Medium-High	Low	Medium-High
		Stockbrokers	Medium	Low	Medium
Insurance	Medium	Insurance	Medium	Medium-low	Medium
Other Financial Institutions	Medium-High	Payment services	High	Medium-low	Medium-High
		Lending	Medium-Low	Medium-low	Medium-Low
		Other activities	Medium	Low	Medium
DNFBP	High	Company service providers	High	Low	High
		Lawyers	High	Low	High
		Trustees and fiduciaries	High	Low	High
		Notaries public	Medium-High	Low	Medium-High
		Accountants and auditors	Medium-High	Low	Medium-High
		Real estate agents	Medium-High	Low	Medium-High
		Dealers in high value goods	Medium	Low	Medium
Gaming	Medium-High	Land based gaming	Medium	Medium-low	Medium-Low
		Remote gaming	High	Low	High

NRA 2018 outcomes (cont.)

TF threat

Overall TF threat	Medium-High

1. Malta's **geographic location** exposes the country to terrorist organisations in neighbouring countries
2. **Influx of refugees from neighbouring countries** could be exploited by terrorist organisations leading to the possibility of terrorist organisations to infiltrate the EU
3. **Cross-border cash transactions** and high levels of remittances, pose a threat due to the difficulty of monitoring money flows

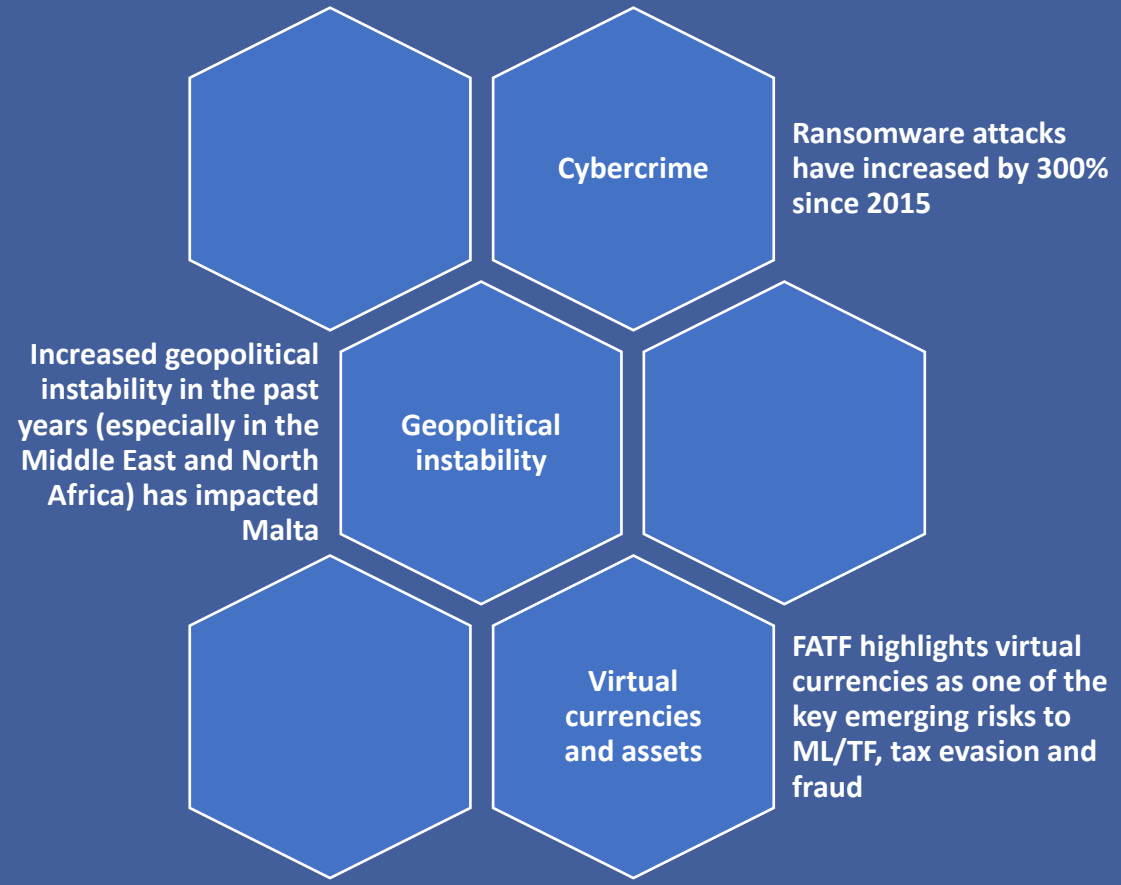
TF vulnerability

Overall TF vulnerability	Medium-High

1. A **lack of transparency** exists in the NPO sector with no obligations for NPOs to register or report financial information[1]
2. There are **weaknesses in controls of cash movements** at sea terminals and airports
3. Persons intending to finance terrorism can take advantage of **lack of oversight** of certain complex products and transactions

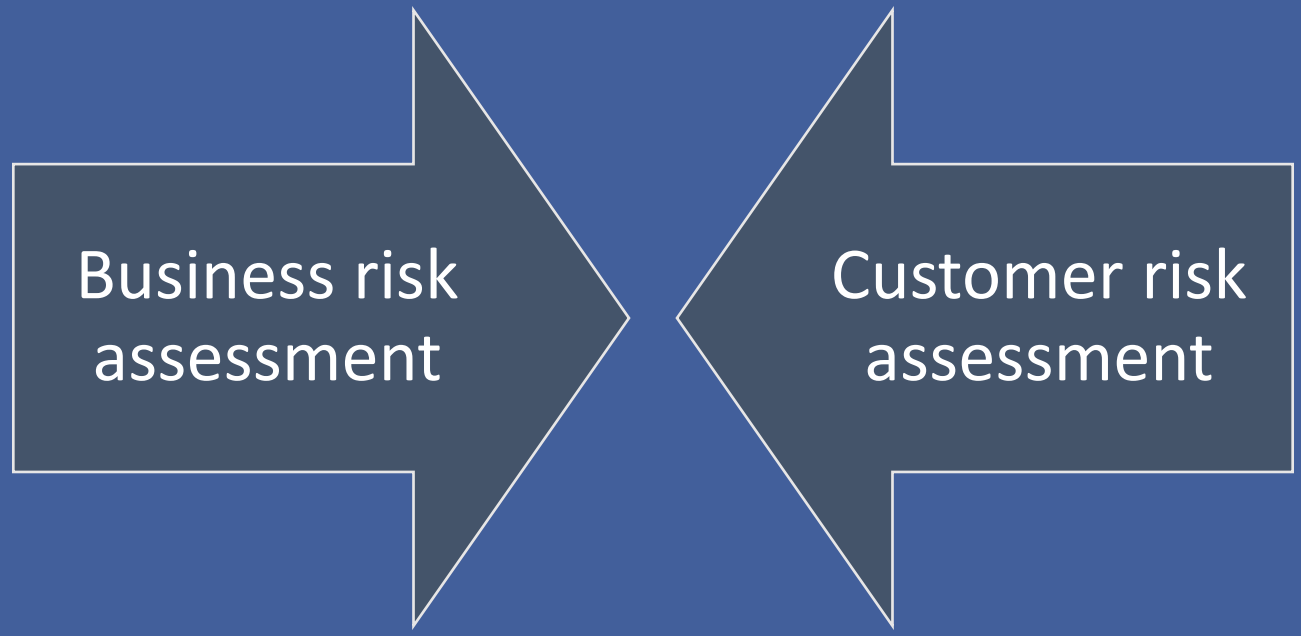
NRA 2018 outcomes (cont.)

Cybercrime, geopolitical risk and virtual currencies all pose potential ML/TF risks to Malta

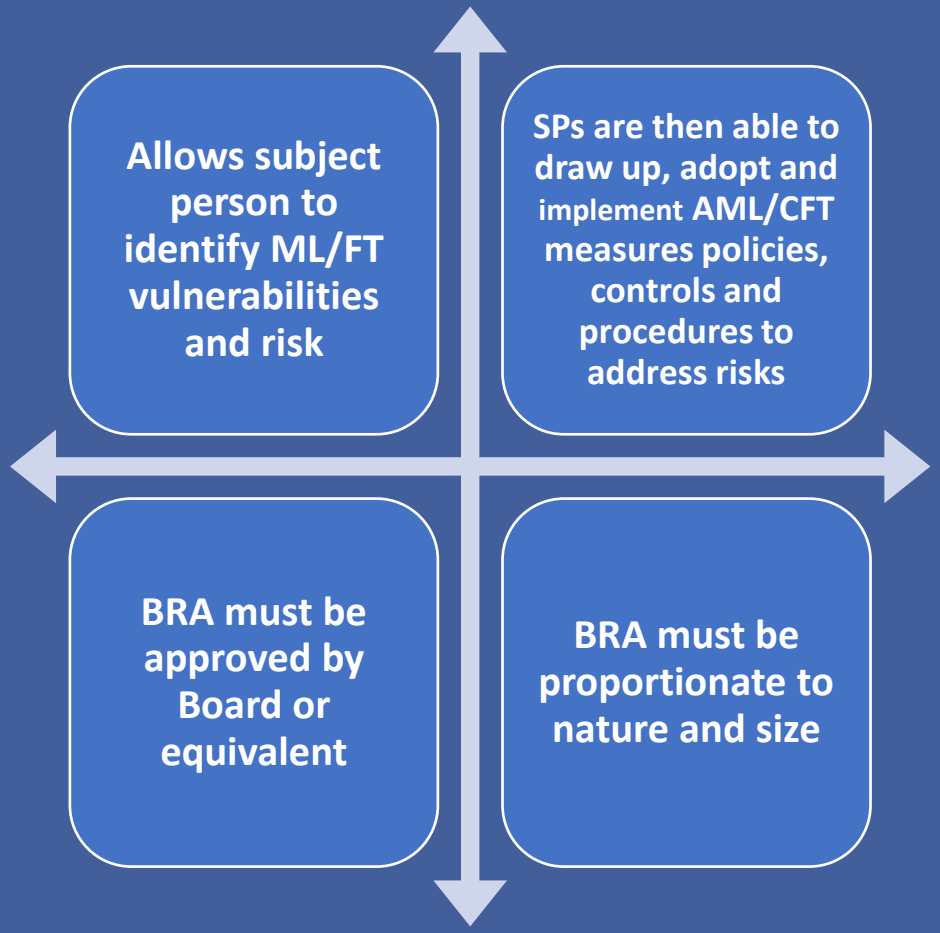


CAMILLERI PREZIOSI
ADVOCATES

Entity-level risk assessment



Business risk assessment



Carrying out the BRA

The following aspects must be covered:

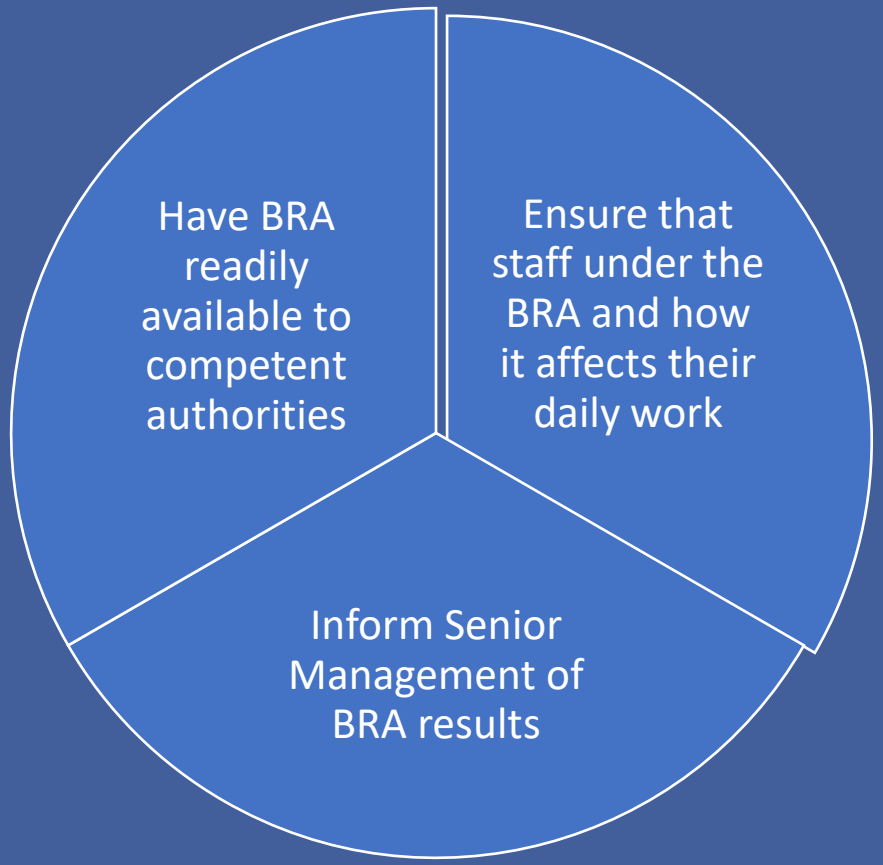
- The methodology adopted by the subject person
- The reasons for considering a risk factor as presenting a low, medium or high risk
- The outcome of the BRA
- Any information sources used

- The more complex the activities the more in depth the risk assessment should be.

  - Eg. A large business conducted through multiple branches, agencies and subsidiaries is less likely to know its clients personally and therefore a more sophisticated risk assessment would be expected.

Implementation of BRA

Firms should:



1. Risk identification/Data Collection

Customer risk	Geographical risk	Product / service / transaction risk	Delivery channel risk
• **Number of customers within each risk factor** • **Maturity of client base, i.e. duration of relationship** • **Volume of business**	• **Number of customers and / or BOs from a given jurisdiction** • **Number of transactions to/from a given jurisdiction**	• **Number of products, services and transactions** • **Customers per each product and service**	• **Number of non-face-to-face relationships** • **Number of introducers and intermediaries**

1. Risk Identification/Data Collection

New and existing technologies

- Monitoring software
- Screening software
- Remote onboarding solutions

Outsourcing Arrangements

- AML/CFT related functions
- Sanction screening
- Audit function
- Identification
- Verification

Internal controls-related vulnerabilities

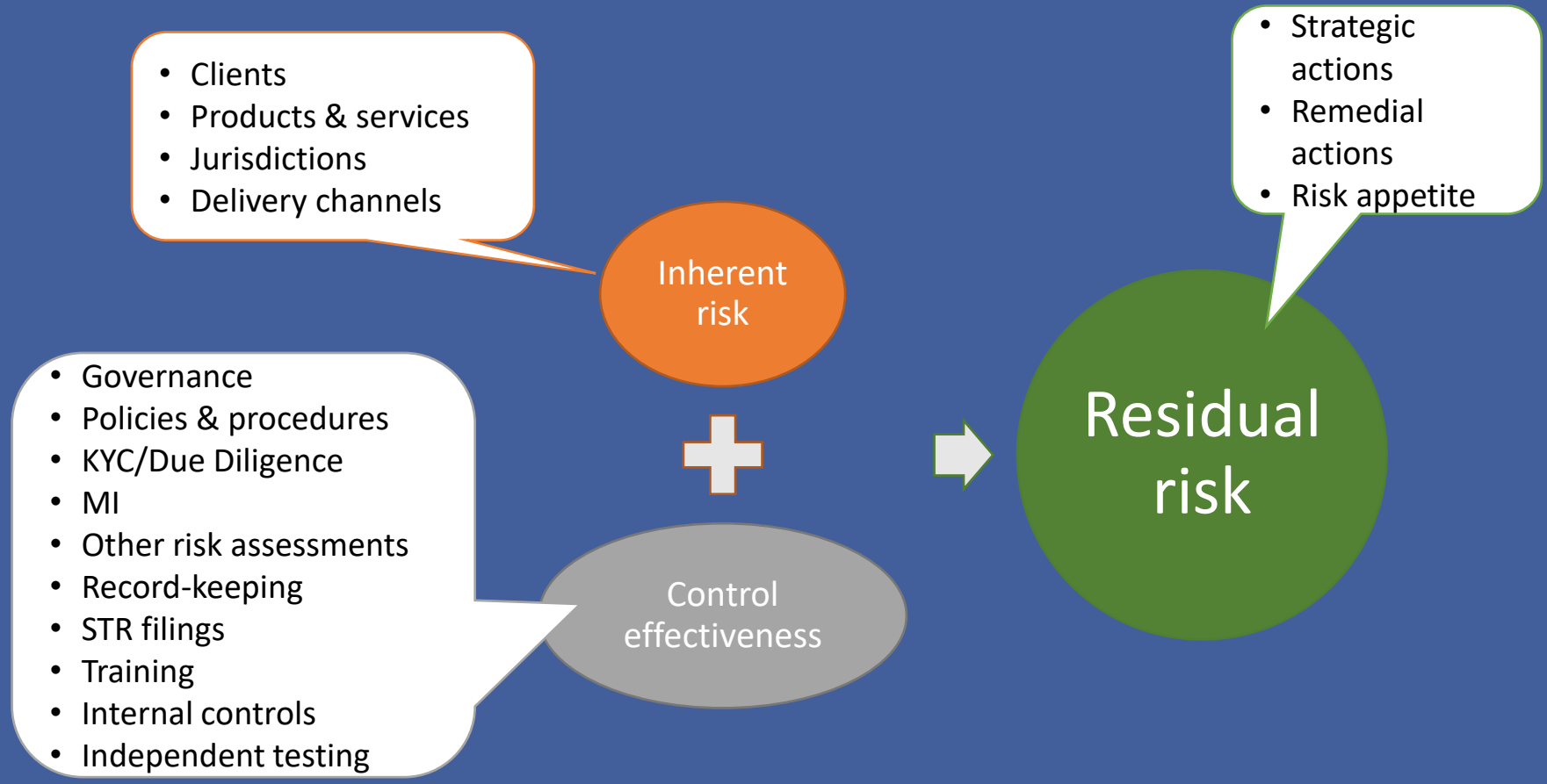
- Governance
- ML/FT risk management control (inc.audit quality and findings)
- Resources (human, technical, financial etc)
- Preventive measures/controls implementation

2. Risk assessment / measurement

- Subject persons will have to **examine** their business structures, client-base and portfolio of services, as well as plans in the pipeline that they may have which would alter their ML/FT risk profile

- Once the subject person would have identified the threats it is exposed to and the vulnerabilities that may be exploited for ML/FT purposes, the subject person will have to determine the **likelihood** of any one scenario materialising itself, and the possible **impact** thereof.

2. Risk assessment/measurement



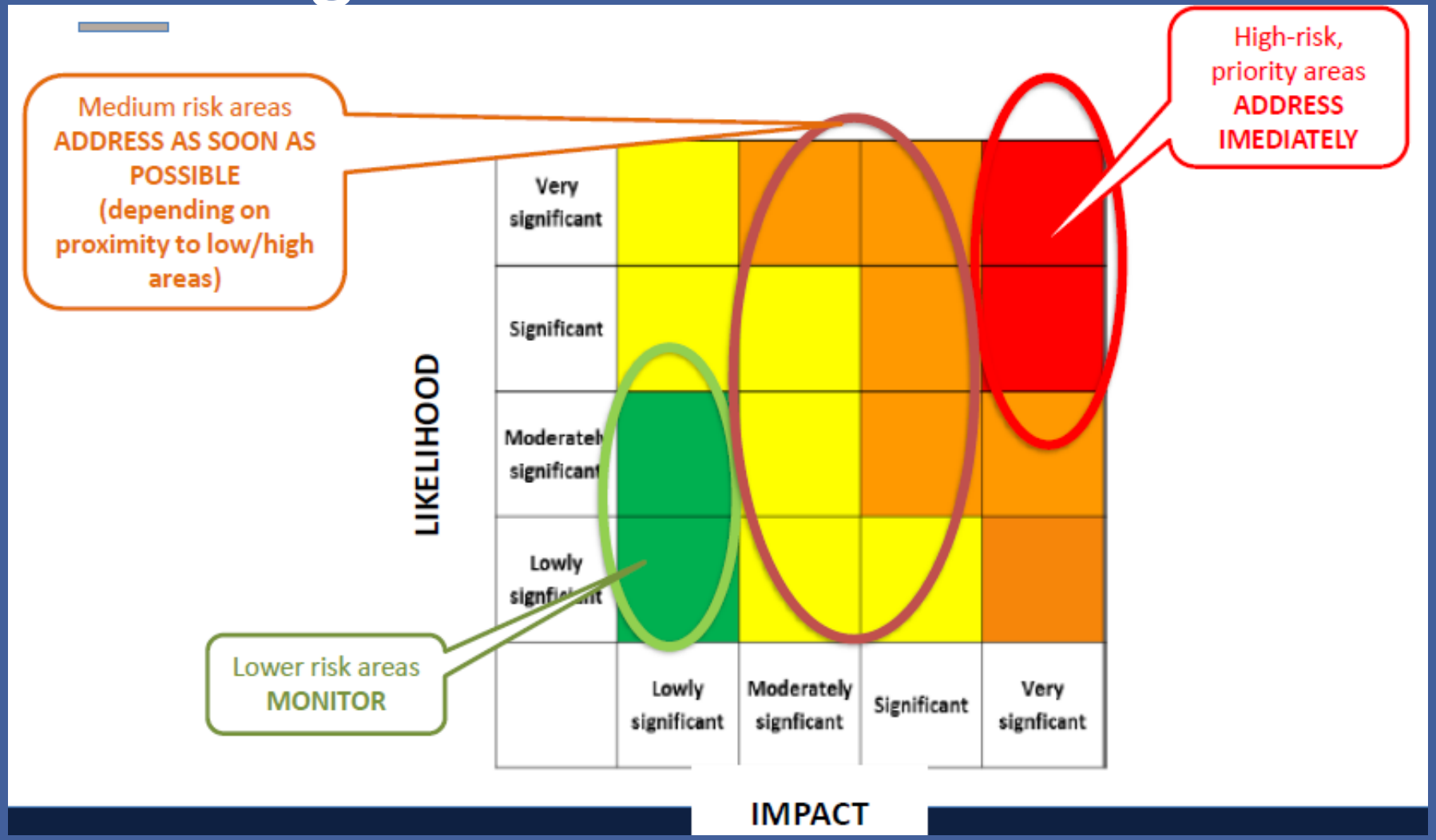
3. Risk Control/Management

- Approval of the assessment results by higher management;
- Board of directors or similar type of management body

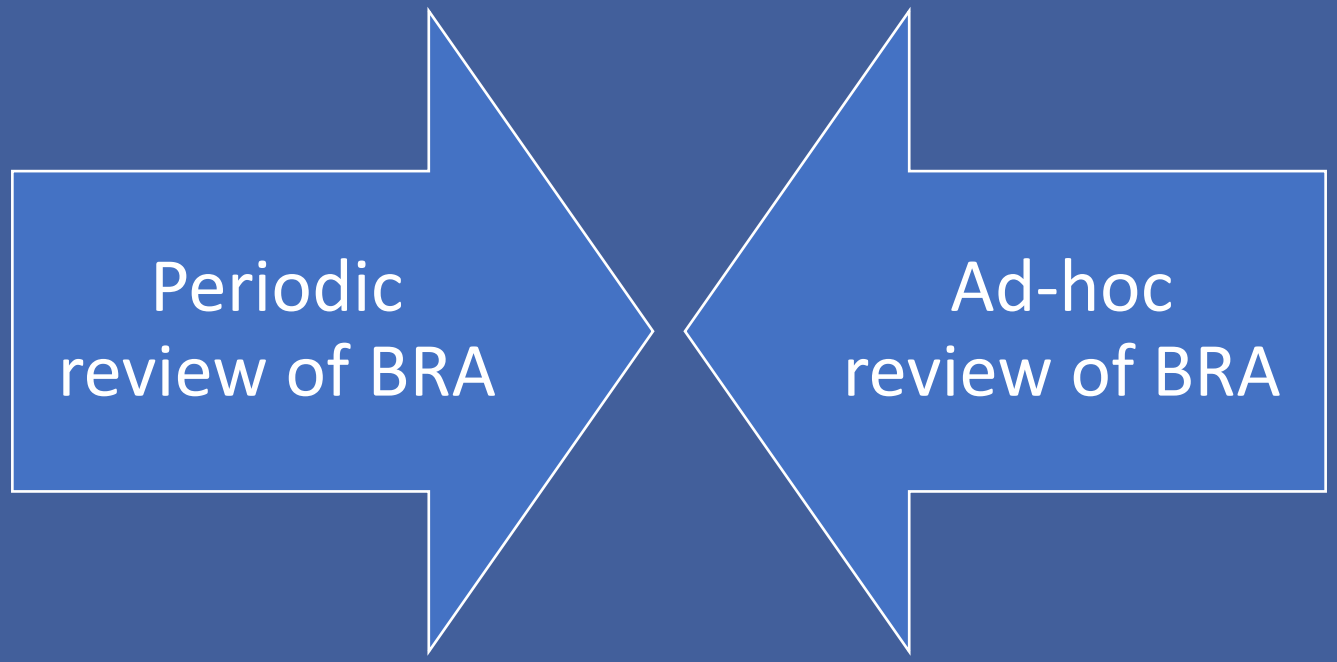
- Approval of an action plan to mitigate the risk
  - Allocation of responsibilities, timelines etc;
  - What are you going to do to mitigate the risks?;
  - Action plan must be approved by senior management
    - Why? Management is a decision-making body and most of the time more resource would be needed to implement measures

Manage the identified ML/FT risks by applying measures, policies, controls & procedures which minimise as much as possible the identified risk

3. Risk Management



4. Continuous Risk Monitoring and Review



Monitor, review and keep update the BRA. Document the assessment process & any updates to the BRA & corresponding AML/CFT measures, policies, procedures & controls

What triggers and ad-hoc review?

- **Major developments in risk management and operations**
  - Change of business model
  - Material and significant changes in client base and clients' operations
  - Use of new technologies
  - Use of new delivery channel methods
  - Unjustified or significant increase/decrease in STRs files according to the firm's risk profile
  - Significant operations in/with high risk countries and/or clients from high risk countries
- **Unexpected events**
  - International scandals (eg. Panama Paper/Pandora leaks)
  - Adverse information from sources (eg. Media reports)
  - Information from a whistle-blower
  - Feedback from the supervisors and other competent authorities (FIU, State, Security, Police etc)
  - Reports from international/national bodies
  - Developments of the legal framework
  - Relevant changes in risks present in Malta (eg. Arising from NRA)

4. Risk monitoring & review

- Documentation – made available to supervisory authorities on request:
  - Methodology for BRA
  - Reasons for scoring risk factors
  - Outcome of BRA, including measures, policies, procedures and controls
  - Information sources
  - Approval levels

- Subject persons are to review their BRA:
  - When new threats and vulnerabilities are identified
  - When there are changes to the business model/structure/activities
  - When there are changes to the external environment within which the subject person is operating
  - At least on an annual basis

The BRA and changes thereto are to be approved by the Board or equivalent

How to integrate national/sectoral risk assessment into BRA?

High level of corruption in a country:

- Enhanced monitoring;
- Each transaction should be scrutinized;
- Specific focus on close associates and BOs, etc

Prevalent use of cash in a country

- Examine clients and transactions database;
- Focus on customer engaged in cash intensive business;
- Conduct retrospective monitoring of all cash transactions to identify patterns;
- Enhanced monitoring scenarios for payments in physical cash (review threshold, require supporting documentation)
- Scrutinize SOW/SOF
- Subject clients that are engaged in cash intensive business to EDD measures

Mitigating Risk

- Once a subject person has identified the ML/FT risks it is exposed to, it must take measures to prevent such risks from materialising or at least mitigate their occurrence as much as possible.

- By virtue of Article 5(5) of the PMLFTR, a subject person must have certain measures, policies, controls and procedures in place to address the risks identified, and such are to include:

a) CDD, record-keeping procedures and reporting procedures;
b) Risk management measures, including CAPs, CRA procedures, internal controls, compliance management, communications and employee screening policies and procedures.

Lessons learnt on the BRA from FIAU enforcement measures

Consider threats and vulnerabilities	Consider likelihood of risks materialising (i.e. scenarios) & their impact	Assess the mitigating effect of control measures to determine level of residual risk
Prepare jurisdictional risk assessments	Be as detailed as possible in the documentation	Evidence of discussion & approval at board level

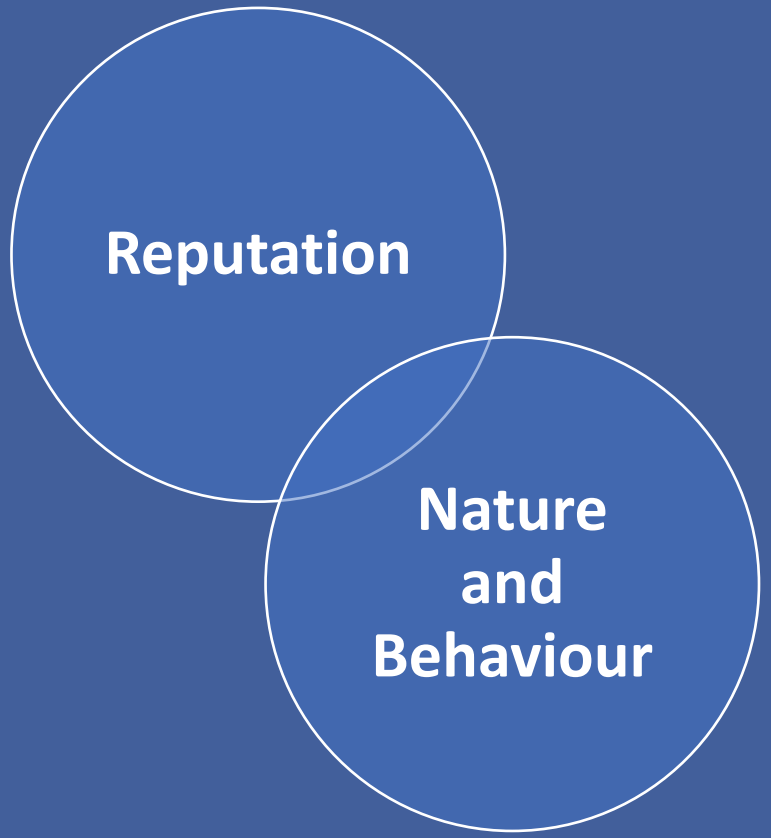
Customer risk assessment

- This assessment allows the subject person to identify potential risks upon entering a **business relationship** with, or carrying out **an occasional transaction** for, a customer.

- It allows the subject person to develop a risk profile for the customer and to categorise the ML/FT risk posed by each customer as low, medium or high.

- The level of detail of a CRA is to reflect the complexity of the business relationship or occasional transaction to be entered into.

Customer Risk Factors



Timing of CRA

- CRA must be carried out whenever a new business relationship is to be entered into or an occasional transaction is to be carried out. However, given that the risk is dynamic, in relation to a business relationship, the CRA should be reviewed from time to time.

- The methodology adopted has to be consistent with the risk factors included in the BRA and apply the conclusions reached by the same. Thus, every decision relating to the methodology applied must be documented.

Non-exhaustive list of high-risk factors

Customer risk	Geographical risk	Product / service / transaction risk	Delivery channel risk
• Overly secretive or evasive • False documentation • Criminal connections • SoF/SoW information not commensurate with customers' profile • PEP links • Sanctions • Employment status and industry • Complex structure • Has benefitted from or applied for residency schemes	• Transfers to a high-risk jurisdictions with no apparent connections • Links to high-risk jurisdictions	• Large financial transactions with no apparent economic rationale • Transactions involve recently-created companies • No justification for the transactions being proposed • ML/FT risk presented by the product/service itself	• Multiple intermediaries without good reasons • Use of third parties without good reasons • Non-face-to-face without sufficient controls

Non-exhaustive list of low-risk factors

Customer risk	Geographical risk	Product / service / transaction risk	Delivery channel risk
• Listed entity • Entity operating in the regulated financial business • Client accounts • Government-owned entities	• EU/EEA Member States • Links to jurisdictions which are considered to be reputable and have an equivalent AML/CFT regime	• Use of product/service has been tested • Product does not allow anonymity • There are controls around the product, e.g. capping	• Face-to-face • Use of regulated intermediaries

Sources of Information

- any relevant reports issued by the FATF, MONEYVAL and other bodies;
- reports, typologies and other information made available by FIUs or law enforcement
- agencies;
- sectoral risk assessments;
- information, reports and guidance made available by the ESAs and competent authorities;
- information from industry or professional bodies;
- information from civil society, such as corruption indices and country reports;
- information from international standard-setting bodies, such as mutual evaluation reports or legally non-binding blacklists;
- information from credible and reliable open sources, such as reports in reputable newspapers;
- information from credible and reliable commercial organisations, such as risk and intelligence reports;
- information from statistical organisations and academia; and
- existing experience in providing own products/services.

FIAU risk scoring grid

	Scoring	Type of customer	Product / Service	Interface	Geographical connections
Very high	9-10	• Unregulated virtual currency exchanges • Corporate structures involving the use of bearer shares	• Services intended to render the customer anonymous	• Non-face-to-face through intermediaries	• Country subject to sanctions, embargoes
High	6-8	• Non-Profit Organisations sending funds to non-reputable / high-risk jurisdictions • Correspondent banks • Fiduciary arrangements	• Internet-based products • Services or products identified as posing a high risk of ML/FT	• Non-face-to-face using other means with no embedded technological safeguards	• Non-reputable / high-risk jurisdiction
Medium	3-5	• Highly-paid employees • Public figures • General public	• Retail products	• Non-face-to-face using technological systems with embedded safeguards	• Reputable jurisdiction
Low	1-2	• Other individuals (e.g. pensioners, average-salaried employees)	• Products with very limited transaction / deposit thresholds	• Face-to-face	• EU Member State • Domestic

FIAU risk score

Rating	Impact of ML/FT risk
Very high	Materialisation of risk may have very dire consequences *Response: Do not establish business relationship or allow transaction to occur, or else reduce the risk to acceptable level*
High	Risk likely to happen and/or to have serious consequences *Response: Do not allow transaction until risk reduced*
Medium	Possible this could happen and/or have moderate consequences *Response: May go ahead but preferably reduce risk*
Low	Unlikely to happen and/or have minor or negligible consequences *Response: Fine to go ahead*

Weighting and rating of risk factors

- Taken together, the scores assigned to the individual risk factors should allow the subject person to generate an overall risk score and lead it to understand whether the business relationship or occasional transaction falls within its risk appetite

- The method used to weight risk factors is left to the subject person, provided that the following principles are followed:

  - **Weighting is not to be unduly influenced by just one factor;**
  - **Monetary considerations are not to influence the risk rating;**
  - **PMLFTR default high risk situations are not to be over-ruled (e.g PEPs);**
  - **Weighting does not lead to a situation where it is impossible for any relationship or transaction to be classified as high risk.**

Lessons learnt on the CRA from FIAU enforcement measures

- Requirement for a comprehensive methodology
- Importance of understanding the risk even in the case of reliance
- Documented methodology and scoring system
- Timing of CRA
- CRA must include all risk factors

De-risking and Financial Inclusion

- ‘De-risking’ refers to a decision taken by firms to no longer offer services to some categories of customers associated with higher ML/TF risk.

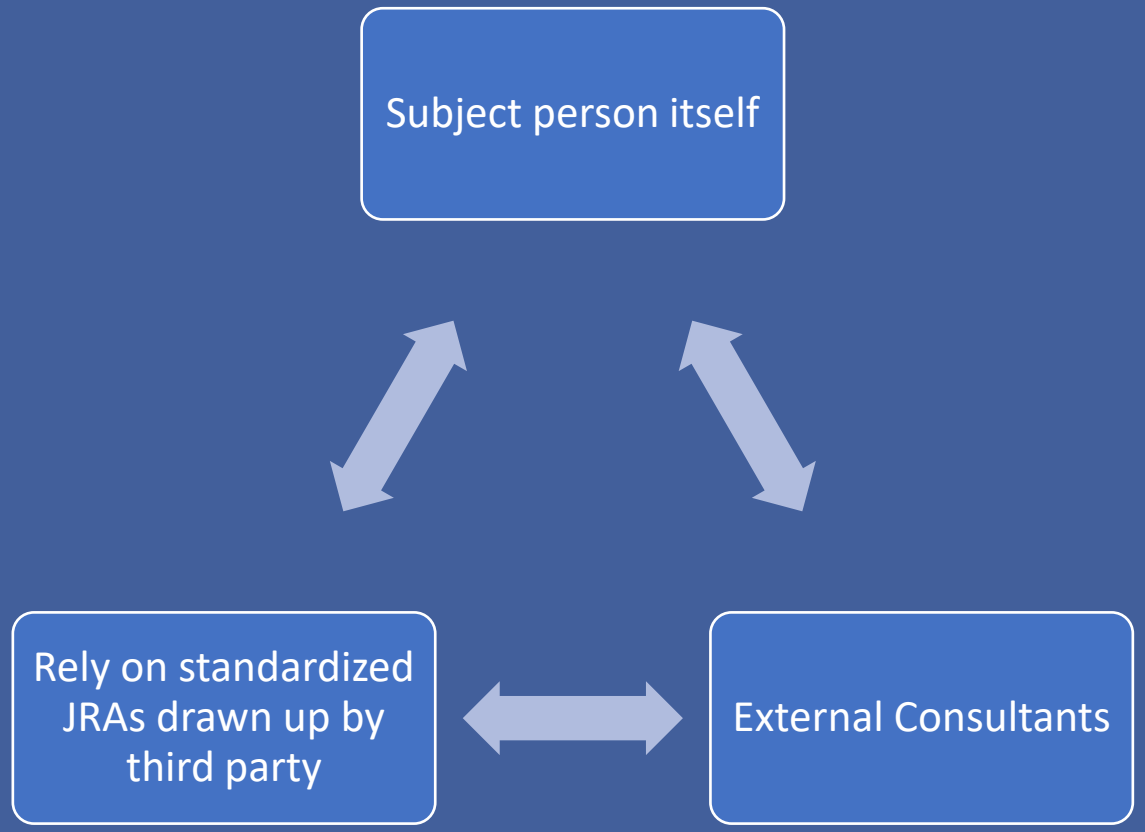
- As the risk associated with individual business relationships will vary, even within one category, the application of a risk-based approach does not require firms to refuse, or terminate, business relationships with entire categories of customers that are considered to present higher ML/TF risk.

- Firms should instead carefully balance the need for financial inclusion with the need to mitigate ML/TF risk.

Jurisdictional Risk Assessment (JRA)

- Subject Persons are required to carry a JRA with respect to the countries it may be exposed to ML/FT risk;
- The assessment should highlight the main risks connected with the specific jurisdiction;
- Similar to the BRA, the detail included should be proportionate to the nature and size of the business and its exposure;
- There is no one size fits all approach expected for EU member states
- To take into consideration the customer activity, including business activities, SOW and SOF to determine the SP's geographical risk exposure

Who can carry out a JRA?



CAMILLERI PREZIOSI
ADVOCATES

Factors and Sources

- Level of Transparency & Rule of Law (e.g., of source/s include *World Justice Project Rule of Law Index, Freedom in the World* and *Freedom of the Press,* issued by Freedom House;
- Level of Corruption (e.g., of source/s include *Corruption index,* issued by Transparency International);
- War-torn countries/Civil unrest (e.g., of source/s include *UN list of Embargoed Countries*);
- Significant level/s & type/s of crime/s (jurisdictions known for high level of different types of crimes, including drug trafficking, arms trafficking, human trafficking, jurisdictions known to be a hub for terrorist groups);
- Significant level of terror threat (e.g., of source/s include the *Global Terrorism Index,* issued by the Institute for Economics and Peace);
- Mutual Evaluation Report (MERs) issued by the FATF or any FSRB; and
- Other notable sources (e.g., of source/s include the *Basel AML Index,* issued by the International Centre for Asset Recovery).

JRA Examples

(a) Where a subject person is involved in the processing of payments, its exposure to geographical risk will not be limited to the jurisdictions linked to its customer and beneficial owner but it will also arise from the main jurisdictions from which it is receiving or remitting funds on behalf of its customer. However, attention has always to be paid to the risk of FT which may manifest itself through geographical risk independently of the value and volume of payments remitted to jurisdictions presenting a high risk of FT.

(b) Where a subject person is providing tax advice in relation to a given corporate structure, the geographical risk associated with the jurisdictions where the entities used to channel funds or to exercise control within the said structure are incorporated, registered or otherwise established has to be considered together with the geographical risk linked to the customer and its beneficial owner. The presence of entities incorporated or registered in jurisdictions known to provide favourable tax regimes and that have beneficial ownership transparency issues will inevitably increase the ML risk linked to tax evasion or arising from attempts at shielding the beneficial owners of the said structure.

JRA examples (cont.)

(c) Where the subject person is providing directorship services to a corporate entity, the geographical risk will not be limited to the country of incorporation or registration of the corporate entity itself or that where its beneficial owner is resident but will also arise from those jurisdictions where its main trading partners are located or the assets held by it are located.

(d) Where the subject person is collecting or receiving funds from customers as is the case with collective investment schemes or insurance (intermediary) undertakings, the geographical risk will arise from the jurisdictions where the respective products are being marketed and its customers are resident, incorporated or otherwise established.

Third parties/Consultants considerations

- The risk assessment carried out considers a sufficient number of aspects that may impact the subject person, and the sources used for the purposes of the said assessment are not only known but are also reliable ones. Subject persons can refer to Section 8.1.2. of the Implementing Procedures – Part I regarding reliability.
- In the event that particular aspects are not factored in, then the subject person should supplement the said risk assessment and consider what is likely to be the impact on the risk rating provided by the third party. By way of example, a third party assessment that does not consider the level of terrorism or funding of terrorism to which a jurisdiction is exposed would be of no value to anyone providing money remittance or similar services.
- The subject person must understand the methodology behind the risk assessment and the resulting risk rating attributed to any one given jurisdiction. It has to be ascertained that the said methodology makes sense and is sufficiently objective.
- The subject person has to ensure that any assessment and associated risk rating is updated periodically. In particular, subject persons have to consider how quickly the said assessments and ratings are revised once there are changes in a jurisdiction's circumstances. Events can precipitate quite quickly and what was once a low risk jurisdiction may undergo a drastic change in risk. If the third party risk assessments and associated rating are not revised regularly within a reasonable period of time, the subject person would have to consider and factor in any new information that may become available and that impacts one's risk understanding itself.
- The fact that a subject person may be making use of a readily available index does not absolve the subject person from understanding the main reasons for a jurisdiction being considered as presenting its assigned level of risk, especially in situations where a jurisdiction is deemed to present a higher than usual risk of ML/FT.

EDD measures for non-reputable jurisdictions/high-risk jurisdictions

Subject persons may, with respect to business relationships or occasional transactions involving non-reputable or high-risk jurisdictions, consider applying the following EDD measures:

a) obtain additional information on the customer and on the beneficial owner(s);
b) obtain additional information on the intended nature of the business relationship;
c) obtain information on the source of funds and source of wealth of the customer and of the beneficial owner(s);
d) obtain information on the reasons for the intended or performed transactions;
e) obtain the approval of senior management to establish or continue the business relationship;
f) conduct enhanced monitoring of the business relationship by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination;
g) introduce an enhanced, relevant reporting mechanism or systematic reporting of financial transactions; and
h) limit business relationships or transactions with natural persons or legal entities from non-reputable jurisdictions.

Concluding Remarks

Any questions?

Thank you

Technical Excellence, Practical Solutions

CAMILLERI PREZIOSI
ADVOCATES

INTERLAW.
An International Association of Independent Law Firms