Application of a Risk-Based Approach

8th January 2024

Peter Mizzi

Agenda

- Risk-Based Approach;
- Supranational Risk Assessment;
- National Risk Assessment;
- Business Risk Assessment;
- Customer Risk Assessment; and
- Jurisdictional Risk Assessment.

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/CFT 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.

CAMILLERI PREZIOSI
ADVOCATES

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 2022 Outcomes

Sector	Main risks
Cash and cash-like assets	• Privately owned ATMs presents new opportunities for organised crime groups to enter the financial system in a relatively undetected fashion. • Remains popular despite the pandemic and technological developments due to the anonymity and ease of movement
Financial sector	• Lack of clarity and consistent rules • Credit/payment institutions, bureaux de change, e-money institutions and credit providers are all prone to being misused for ML/FT purposes
Non-financial sector	• Difficulties in identifying Beneficial Ownership • Abuse of shell companies; • Low STR reporting • Real estate sector and tax-related crimes are of high ML/FT risk
Gambling sector	• Exchangeable tokens used in video games were likened to crypto-assets and therefore the risk are perceived to be similar
NPOs	• Becoming less attractive due to rigid due diligence obligations
New products / services	• Transparency over player transfers and club ownership required to mitigate ML/FT risk with professional football • Luxury free ports identified as being of high risk • Investor citizenship and residence schemes

SNRA – Mitigating Measures

- In light of the above, the Commission noted various proposed legislative mitigating measures, such as the implementation of a regulation establishing a new **EU AML/CFT Authority and the introduction of a single AML/CFT rulebook,** which obliged entities would do well to familiarise themselves with in order to keep track and gear up for implementation of such measures.

- All in all, the main takeaway by obliged entities ought to be that the findings of the SNRA should be understood and observed in light of their risk appetite and the products and services which they provide. Obliged entities should then attempt to update their AML/CFT policies, procedures, and controls accordingly, albeit following a risk-based approach, and conduct internal training to ensure that new emerging risks are fully understood and where possible, mitigated.

2018 NRA vs 2023 NRA

Risk assessment	2018 NRA residual risk	2023 NRA residual risk
Money Laundering – residual risk		
Financial sector		
Banking	Medium-high	Medium
Financial Institution	Medium-high	Medium-high
Investment services	Medium-high	Medium
Pensions	Medium	Medium
Insurance	Medium	Medium-low
DNFBPs		
Gaming		
Remote gaming	High	Medium
Land-based gaming	Medium-low	Medium
Recognition notice framework	N/A	Medium-high
CSPs	High	Medium-high
Accountants and auditors	Medium-high	Medium
Lawyers	High	Medium
Tax advisors	N/A	Medium-high
Dealing in immovable property	Medium-high	Medium-high
High value goods	N/A	Medium-high
VFAs and VFASPs*		Medium
Other instruments - ML residual risk		
Legal persons	High	Medium-high
Legal arrangements	High	Medium
Citizenship & residency by investment schemes	N/A	Medium
NPOs (Voluntary Organisations)	High	Medium
Terrorism Financing**		Medium
Proliferation financing and Targeted Financial Sanctions related risks	N/A	Medium

2023 NRA – Proceeds of Domestic Crime

The analysis of the 2023 NRA found that the following predicate offences are the main threats for laundering of proceeds of domestic crime in Malta:

Table 87: Rating of ML threats of domestic proceeds of the most significant crime

Drug trafficking	Medium-high
Organised crime	Medium-high
Fraud	Medium
Corruption	Medium
Tax crime	Medium

2023 NRA – Proceeds of Foreign Crime

The following predicate offences are the main threats for laundering of proceeds of foreign crime in Malta:

Table 89: Rating of threats of ML of foreign proceeds of the most significant crime

Organised crime	Medium-high
Tax crime	Medium-high
Fraud (incl. cybercrime)	Medium-high
Corruption	Medium
Drug trafficking	Medium

2023 NRA – Overall Vulnerabilities

This section presents the rating of the vulnerabilities, which focus on the overall AML/CFT/CPF TFS framework (for detailed analysis see sectoral sections).

Table 93: Ratings for the vulnerabilities

Vulnerability in the constitutional framework in the judicial review of sanctions that may impede or undermine supervisors from imposing proportionate, effective, and dissuasive administrative sanctions, including pecuniary penalties.[100]	High
Challenges in monitoring activities of legal persons with no links to Malta[101]	High
De-risking[102]	High
Limited pool of professional human resources	High
Vulnerabilities in the judicial system including the committal proceedings[103], the ML trial without jury, and the virtual evidence and vulnerabilities in relation to selling of assets by the ARB during criminal proceedings	High
Lack of criminal defence regime protecting subject persons when submitting suspicious reports and there is the appropriate consent from the FIAU	Medium-high
Possible differences between sectoral MLRO approval procedures	Medium-high
Recognition framework for foreign gaming license holders[104]	Medium-high
Obstacles to authorities' cooperating and coordination in enforcement matters	Medium-high
Lack of sufficient and comprehensive criteria for quality of STR reporting	Medium
Vulnerability in fighting tax crime and the collection of taxes	Medium
Short-term of FIAU postponement order[105]	Medium
Harmonised statistics	Medium

2023 NRA – Overall Vulnerabilities

This section presents the rating of the vulnerabilities, which focus on the overall AML/CFT/CPF TFS framework (for detailed analysis see sectoral sections).

Table 93: Ratings for the vulnerabilities

Vulnerability in the constitutional framework in the judicial review of sanctions that may impede or undermine supervisors from imposing proportionate, effective, and dissuasive administrative sanctions, including pecuniary penalties.[100]	High
Challenges in monitoring activities of legal persons with no links to Malta[101]	High
De-risking[102]	High
Limited pool of professional human resources	High
Vulnerabilities in the judicial system including the committal proceedings[103], the ML trial without jury, and the virtual evidence and vulnerabilities in relation to selling of assets by the ARB during criminal proceedings	High
Lack of criminal defence regime protecting subject persons when submitting suspicious reports and there is the appropriate consent from the FIAU	Medium-high
Possible differences between sectoral MLRO approval procedures	Medium-high
Recognition framework for foreign gaming license holders[104]	Medium-high
Obstacles to authorities' cooperating and coordination in enforcement matters	Medium-high
Lack of sufficient and comprehensive criteria for quality of STR reporting	Medium
Vulnerability in fighting tax crime and the collection of taxes	Medium
Short-term of FIAU postponement order[105]	Medium
Harmonised statistics	Medium

2023 NRA – Residual Risk – Predicate Offences

Table 9ii: Residual risk – laundering of the proceeds of crime by predicate offence

Topic	Inherent risk	Effectiveness of mitigating measure	Residual risk level
Laundering of proceeds in Malta from domestic drug trafficking	Medium-high	Substantial	Medium-high
Laundering of proceeds in Malta from local organized crime	Medium-high	Substantial	Medium-high
Laundering of proceeds in Malta from foreign organised crime	Medium-high	Substantial	Medium-high
Laundering of proceeds in Malta from foreign crime: fraud (including cybercrime)	Medium-high	Substantial	Medium-high
Laundering of proceeds in Malta from corruption in Malta	Medium	High	Medium-low
Laundering of proceeds in Malta from domestic tax crime	Medium	High	Medium-low
Laundering of proceeds in Malta from foreign tax crime	Medium-high	High	Medium
Laundering of proceeds in Malta from foreign crime: corruption	Medium	Substantial	Medium
Laundering of proceeds in Malta from foreign crime: drug trafficking	Medium	Substantial	Medium
Laundering of proceeds in Malta from domestic fraud	Medium	Substantial	Medium

2023 NRA – Residual Risk – Typology

Table 97: ML residual risk ratings by typology

Topic	Inherent risk	Effectiveness of mitigating measure	Residual risk level
Abuse of Maltese registered legal persons with no sufficient links to Malta, for ML or concealment of BO	High	Substantial	Medium-high
The use of cash and cash-based businesses	High	Substantial	Medium-high
Trade based ML abusing geographical location and transhipment activity	Medium-high	Substantial	Medium-high
Abuse of complex corporate structures for ML or concealment of BO	Medium high	Substantial	Medium-high
Laundering through high-value movables[180]	Medium-high	Substantial	Medium-high
Laundering through immovable property transactions	Medium-high	Substantial	Medium-high
Abuse of Maltese registered legal persons as conduits in VAT fraud	Medium-high	High	Medium
Cross border cash activity	Medium	Substantial	Medium
Laundering of foreign proceeds of fraud through remote gaming operations	Medium	Substantial	Medium

2023 NRA – Rating of TF Threats

Table 98: Rating of TF threats

Threat	Impact	Likelihood	Threat level
Involvement of Maltese legal persons in TF with no transfers through Malta[115]	Severe	Possible	High
Movement of funds for TF via financial institutions	Severe	Likely	High
Movement of funds for TF via cash cross-border movements	Severe	Possible	Medium-high
Movement of funds for TF via credit institutions	Severe	Unlikely	Medium-high
Raising/Movement of funds for TF via disbursements of VOs (NPOs)	Severe	Unlikely	Medium-high
Trade-based TF	Severe	Possible	Medium-high
Raising/Movement of funds for TF via cryptocurrencies	Severe	Possible	Medium-high
Raising/movement of funds for TF via remote gaming	Severe	Possible	Medium-high
Movement of funds through beneficiaries of Trusts	Severe	Very unlikely	Medium
Involvement of BO in TF with no transfers through Malta	Severe	Very unlikely	Medium
Using TF funds domestically	Severe	Very unlikely	Medium

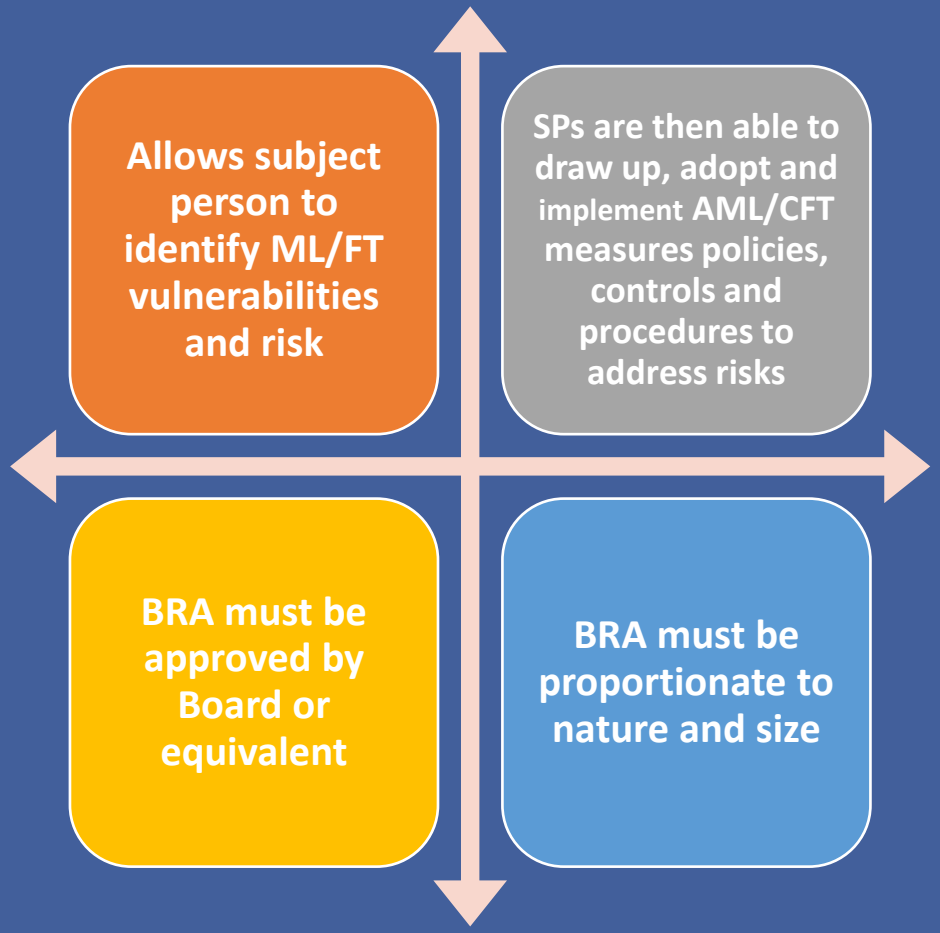
2023 NRA – Rating of TF Vulnerabilities

Table 99: Rating of TF vulnerabilities

Vulnerability	Impact	Likelihood	Vulnerability level
TF lack of understanding of risk by financial remitters	Severe	High	High
Less effective controls in the financial remittance sector	Severe	High	High
Inability to monitor the final destination of cash	Severe	Moderate	Medium-high
Legal persons linked to HRJ which do not bank in Malta	Severe	Moderate	Medium-high
Legal persons linked to HRJ that are not submitting financial statements	Severe	Moderate	Medium-high
Lack of cooperation with countries at a higher risk of terrorism / TF	Severe	Moderate	Medium-high
VOs (NPOs) that fall under the FATF scope level of TF risk awareness	Severe	Moderate	Medium-high
TF lack of understanding of risk by credit institutions	Severe	Low	Medium

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:

CAMILLERI PREZIOSI
ADVOCATES

The 4 stage process

1. Risk identification

- Identify the main ML/FT risks associated with customers, products & services, business practices/delivery channels, & geographical locations

2. Risk Analysis

- Measure the size & importance of ML/FT risks including the likelihood of them materialising and their impact on the subject person

3. Risk Control/Management

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

4. Risk monitoring & review

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

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**

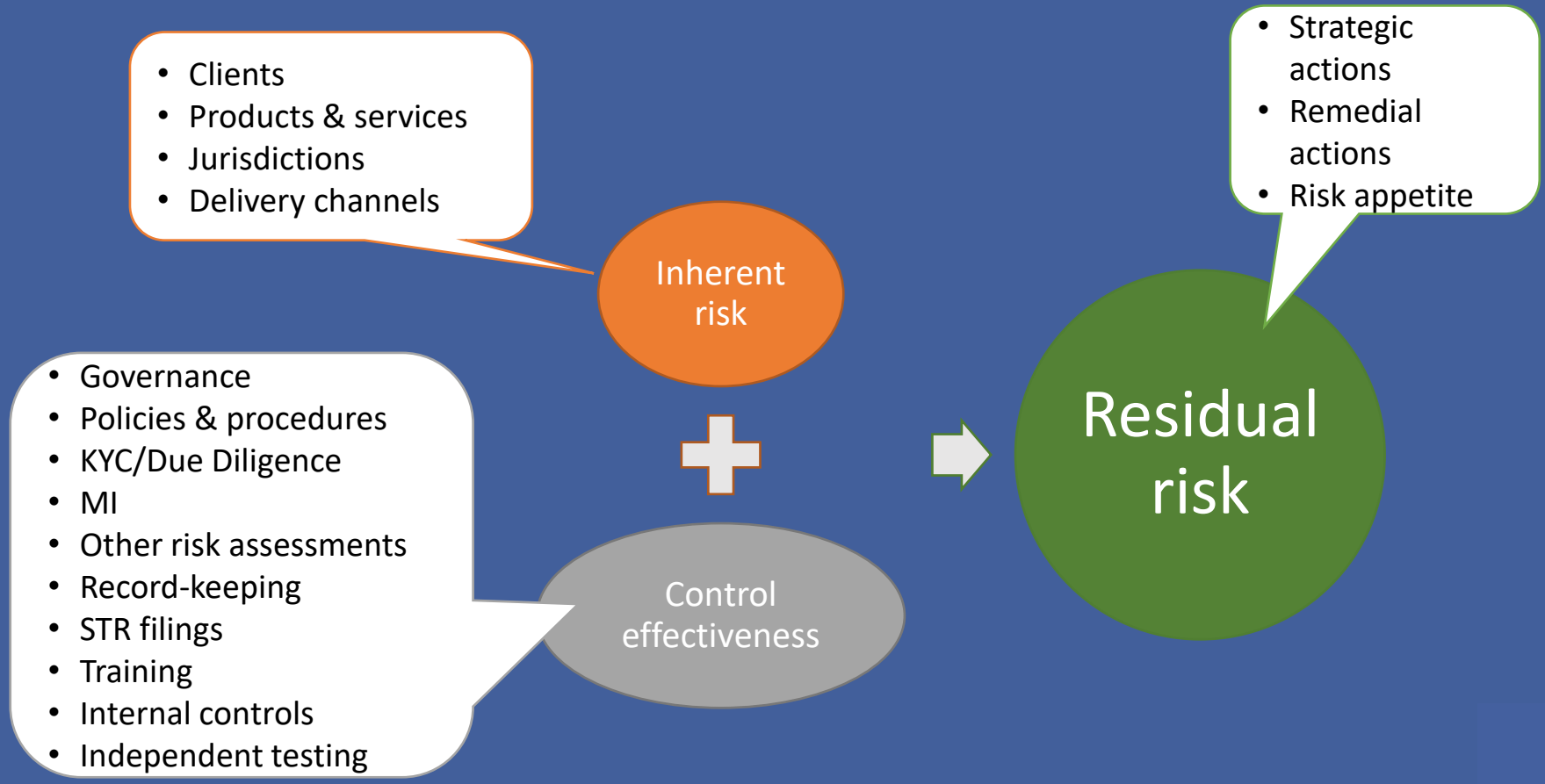
1. Risk Identification/Data Collection

2. Risk Analysis

- 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



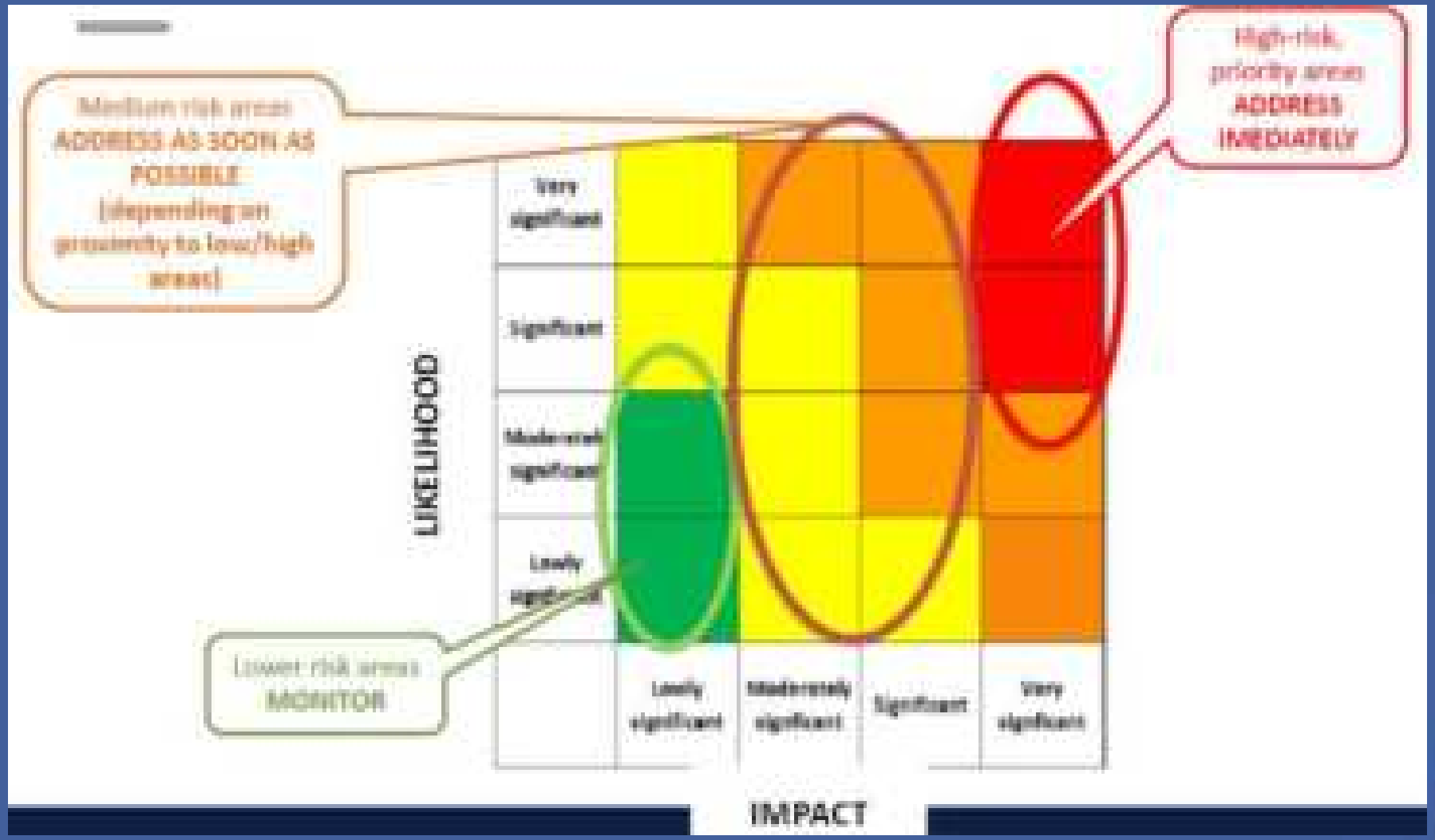
3. Risk Control/Management

- 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

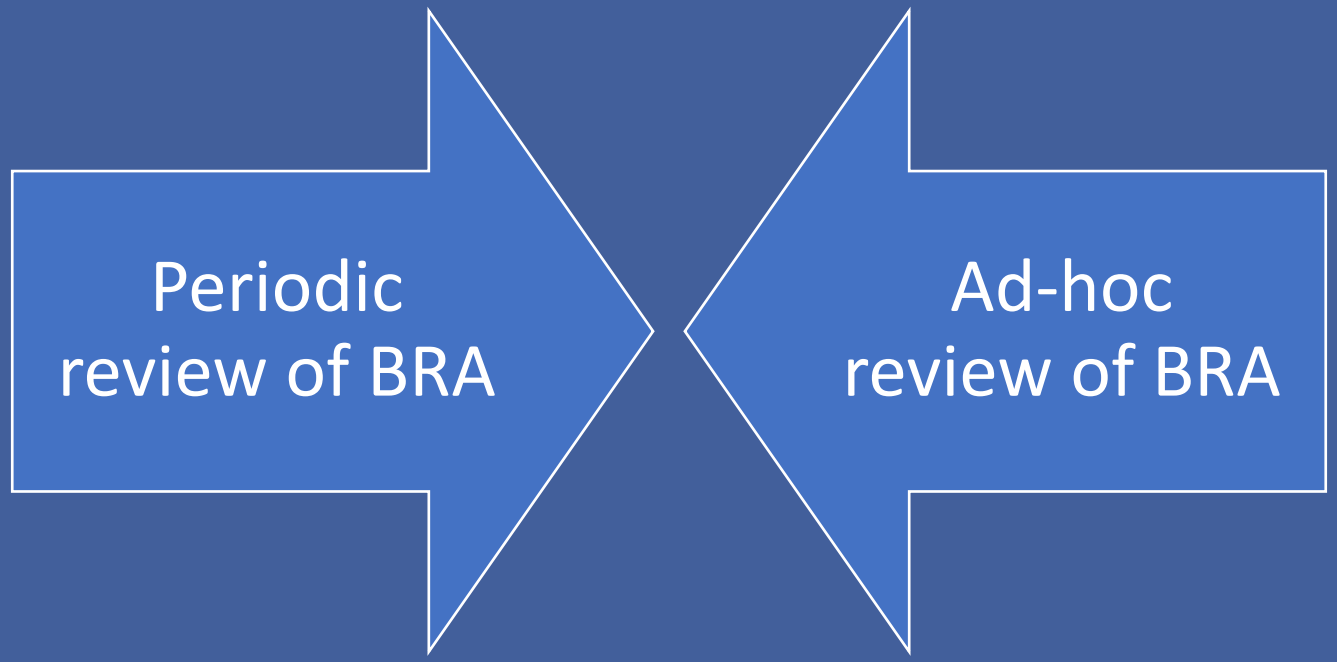


Mitigating Risk

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

- These measures, policies, controls and procedures are to include:
  - CDD, record-keeping procedures and reporting procedures; and
  - risk management measures, including customer acceptance policies, CRA procedures, internal control, compliance management, communications and employee screening policies and procedures.

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 an 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/SNRA)

4. Risk monitoring & review

- 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

BRA good practices

The BRA should be specific to the subject person	Subject persons should understand their own business risk assessment	Subject persons should understand the BRA methodology used	The BRA should include all evident risks that the subject person is exposed to
Generic mitigating measures should be avoided	The calculation of residual risk is essential	The BRA should reflect the actual control & measures adopted	Reference should be made to the National and Supra National Risk Assessment

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

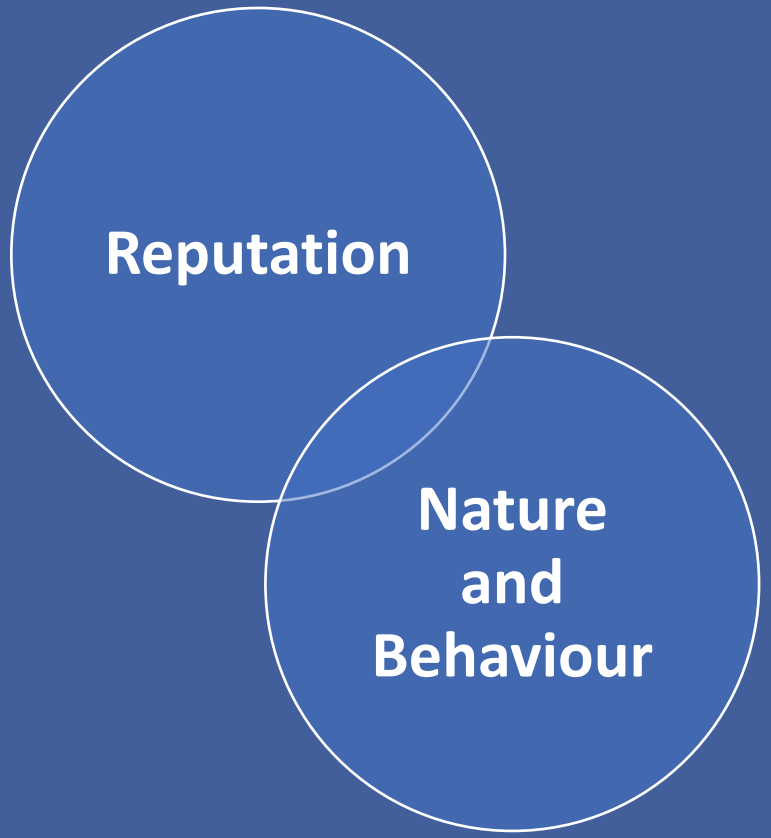
Customer risk assessment

- 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*

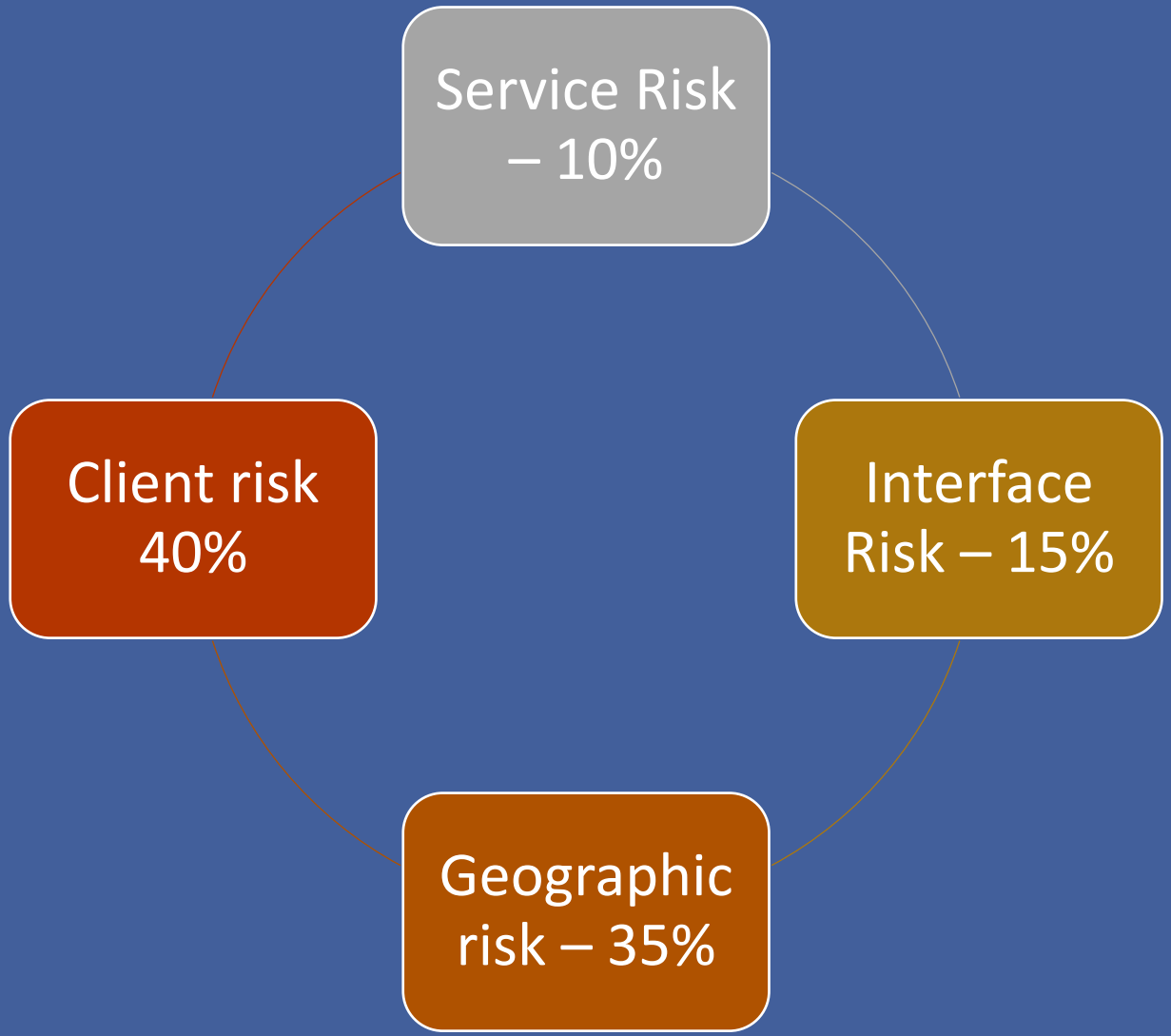
Weighting and rating of risk factors

- 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

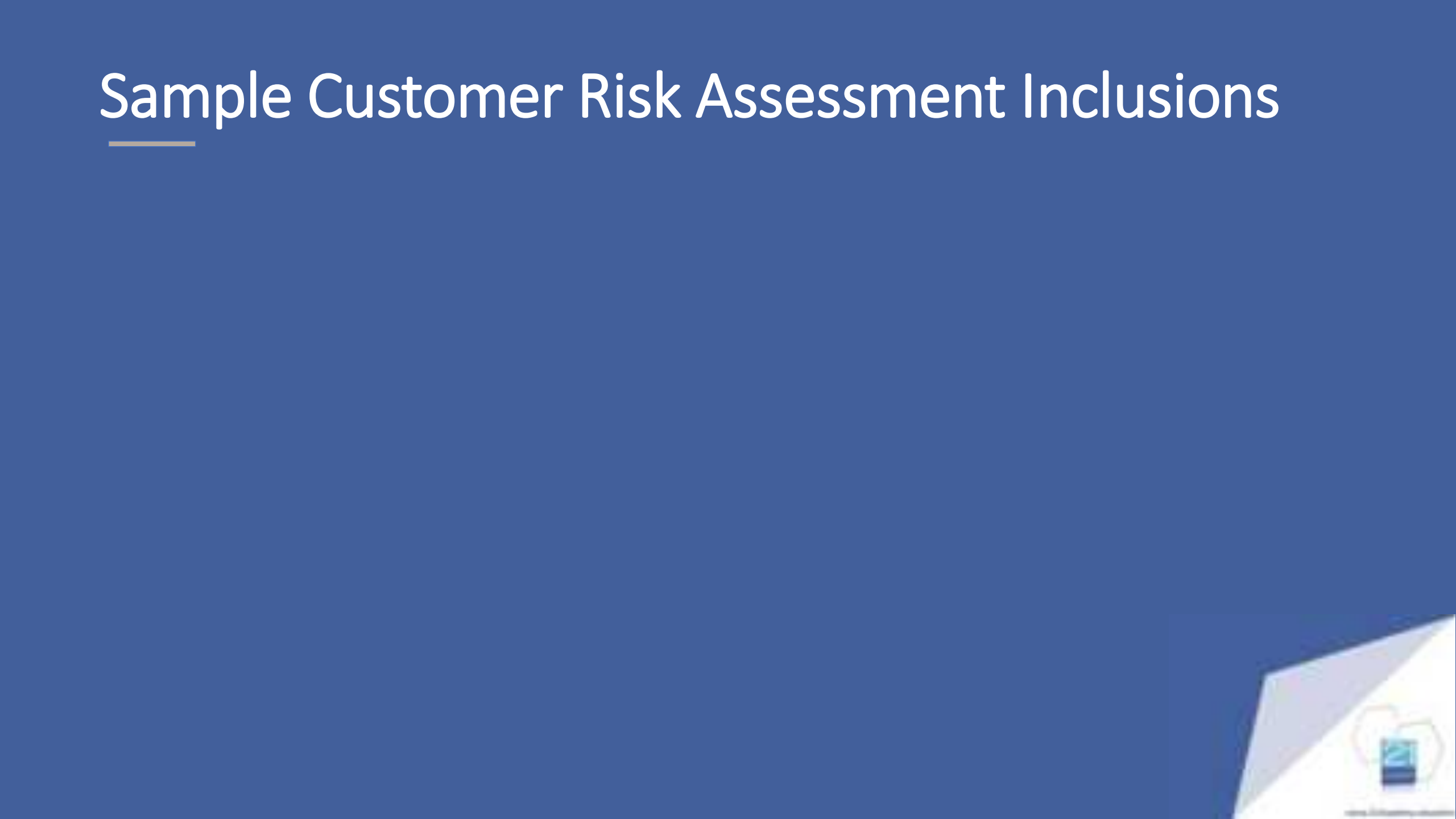
- The method used to weight risk factors is left to the subject person, provided that the following principles are followed:

  - **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.**

Weighting Examples



Sample Customer Risk Assessment Inclusions



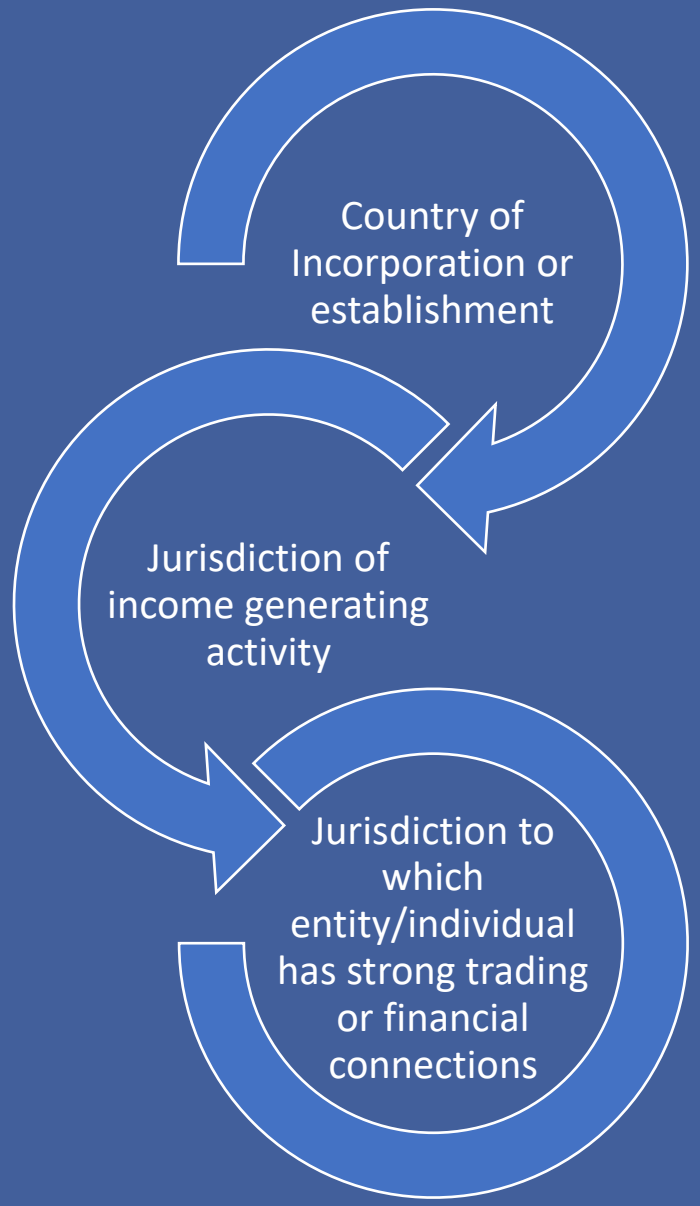
Customer Risk (Legal Persons)

- Is the customer a casino or gaming company?;
- Cash intensive business;
- NGO/Charity;
- Is the customer a listed company?;
- Is the customer established in an EU/EEA jurisdiction?;
- Subject to AML/CFT policies, controls and procedures equivalent to 4th AMLD;
- Opaque/Transparent ownership structure
- Fiduciary/nominee ownership;
- Is the customer a shell company?;
- Is the UBO/director a PEP?

Reputation/Nature & Behaviour Risk Examples

- Reliable adverse information linking the individual to crime (especially financial crime) and/or terrorism;
- Individual subject to UN/OFAC sanctions or EU restrictive measures;
- Reluctant to provide all requested KYC documents without legitimate reasons;
- Doubts exist on the veracity or authenticity of information or documentation provided (included but not limited to KYC);
- Requests for unnecessary or unreasonable levels of secrecy;
- No sound economic and lawful reason for requesting services;
- SoW/SoF is inconsistent with the client's circumstances: client has funds which are obviously or inexplicably disproportionate to their circumstances (e.g. age, income, occupation, or wealth).

Geographical Risk - Examples



Product, Service and Transaction Risk - Examples

Service risk:

- Directorship – sole or co signatory rights (lower risk)
- Directorship – and/or no signatory rights (higher risk)
- Company secretary – lower risk
- Registered office – lower risk

Transaction risk:

- Frequent and unexplained movement of funds between various different entities or geographical locations
- Business relationship conducted in an unusual manner to instructions given in unusual circumstances (as evaluated considering all the circumstances of the client's representation).
- Transactions proposed or effected are complex, unusual, or unexpectedly large or have an unusual or unexpected pattern with no apparent economic or lawful purpose.

Delivery Channel Risk

Face-to-face onboarding;

Non-face-to-face onboarding;

Non-face-to-face onboarding via intermediary/agent – is the intermediary/agent higher or lower risk?

Via reliance

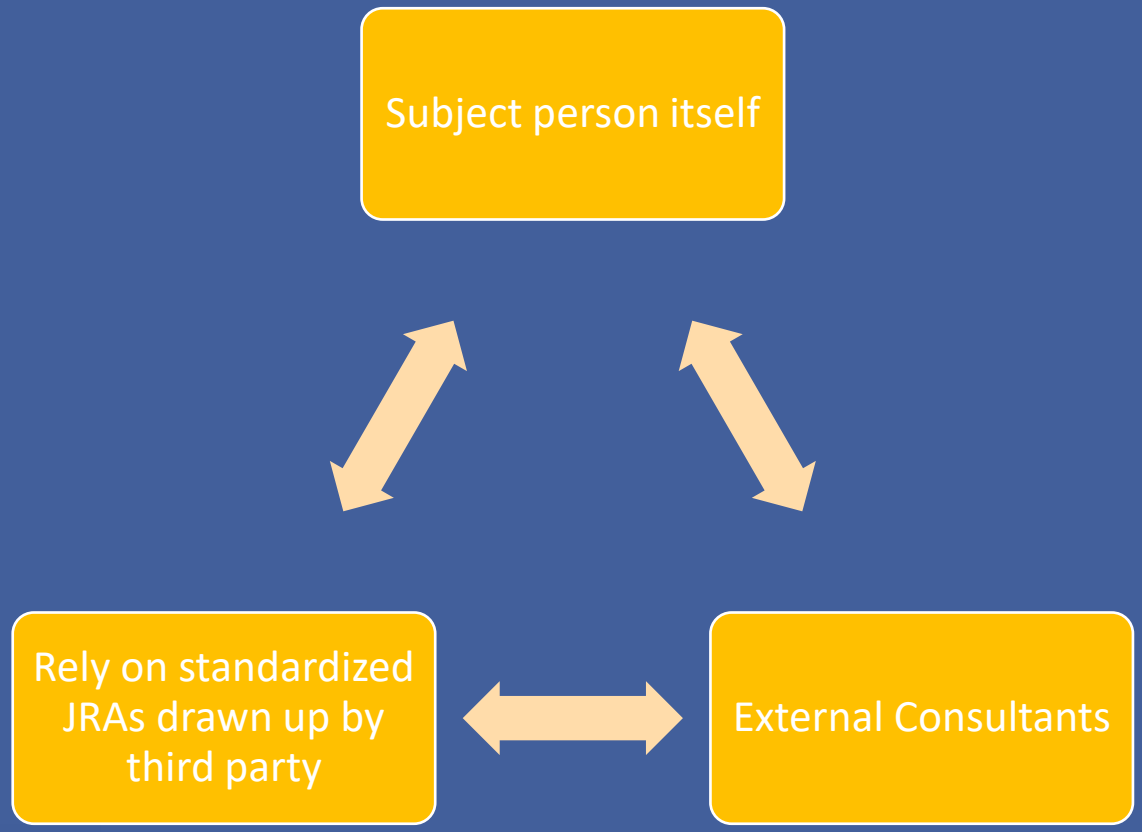
Lessons learnt on the CRA from FIAU enforcement measures

- 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

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?



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

- 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

CAMILLERI PREZIOSI
ADVOCATES

Any questions?

CAMILLERIPREZIOSIADVOCATES

Peter Mizzi

Compliance and AML Advisor

peter.mizzi@camilleripreziosi.com

(+356) 2123 8989

Camilleri Preziosi

Level 3, Valletta Buildings

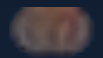
South Street

Valletta, VLT 1103

Malta

THANKYOU

Technical Excellence, Practical Solutions



CAMILLERI PREZIOSI

ADVOCATES

@INTERLAW