www.21Academy.education

Introduction to Anti-Money Laundering (AML) and Funding of Terrorism and understanding the impact of non-compliance

12 November 2020

Diane Bugeja

CAMILLERI PREZIOSI
ADVOCATES

Agenda

- Risk Assessment
- Business Risk Assessment
- Business Risk Assessment Process
- Customer Risk Assessment
- Case Study
- Questions

Risk Assessment

Risk assessment

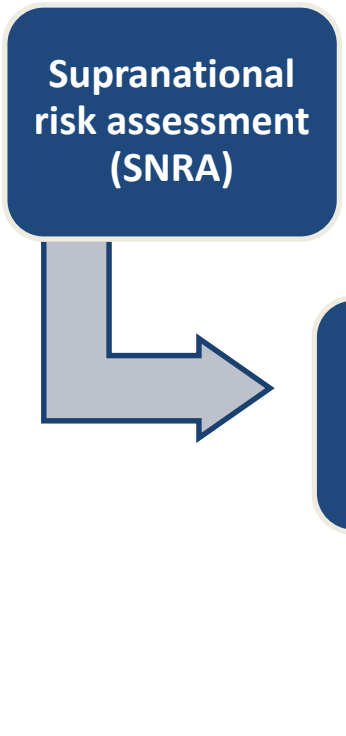
Every subject person shall take appropriate steps, proportionate to its nature and size, to identify and assess the risks of ML/FT that arise out of its activities or services, taking into account risk factors including those related to customers, countries or geographical areas, products, services, 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



- 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

- 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

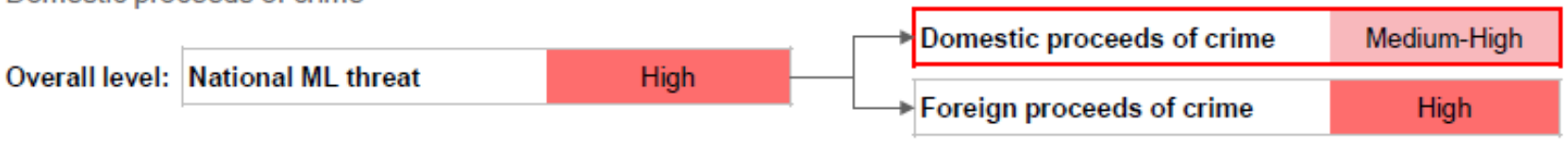
- To be undertaken by the subject person
- Covers ML/TF risks specific to the subject person as well as other broader ML/TF risks which may increase its ML/TF risk exposure

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



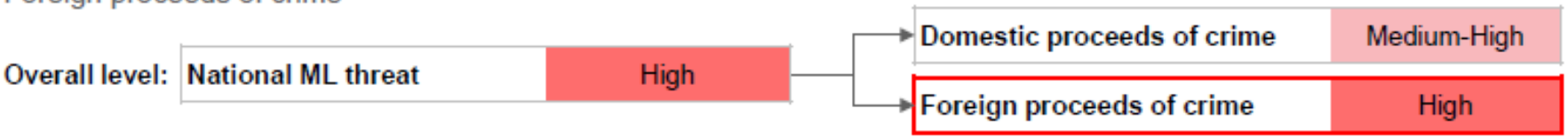
Sub-category	Threat level
Tax evasion	High
Local criminal groups	High
Drug trafficking	Medium-High
Fraud and misappropriation	Medium-High
Corruption and bribery	Medium-High
Smuggling	Medium
Theft and receipt of stolen goods	Medium
Armed robbery	Low
Living of the earnings of prostitution	Low
Usury	Low
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



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

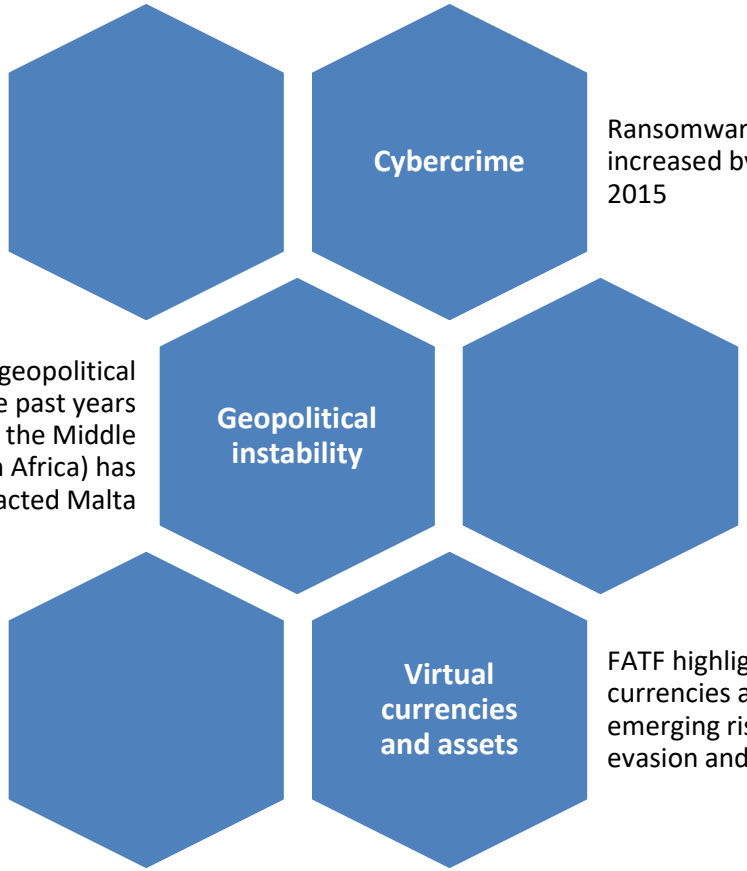
TF vulnerability

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



Entity-level risk assessment

Business Risk Assessment

Business risk assessment

- This assessment allows the subject person to identify its ML/FT vulnerabilities and the ML/FT risks it is exposed to.
- On this basis, subject persons will be able to draw up, adopt an implement AML/CFT measures, policies, controls and procedures that address any identified risks.
- The BRA, any revisions thereof and any decisions taken in relation thereto have to be approved by the Board of Directors or equivalent management body of the subject person.
- External consultants can be engaged to assist but responsibility will always rest with the subject person.
- The BRA must be commensurate to the size and nature of the subject person's business activities and reflect the complexity of same.

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

BRA has to be proportionate to the nature and the size of a subject person's business.

- 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.

Timing of BRA

BRA must be carried out prior to the commencement of activity on the basis of the kind of services, products or transactions it will use to deliver the same and its intended business model and activities.

A subject person should revise and update its BRA:

(A) Whenever new threats and vulnerabilities are identified

(B) Whenever there are changes to its business model/structure/activities

(C) Whenever there are changes to the external environments within which the subject person is operating.

Business Risk Assessment Process

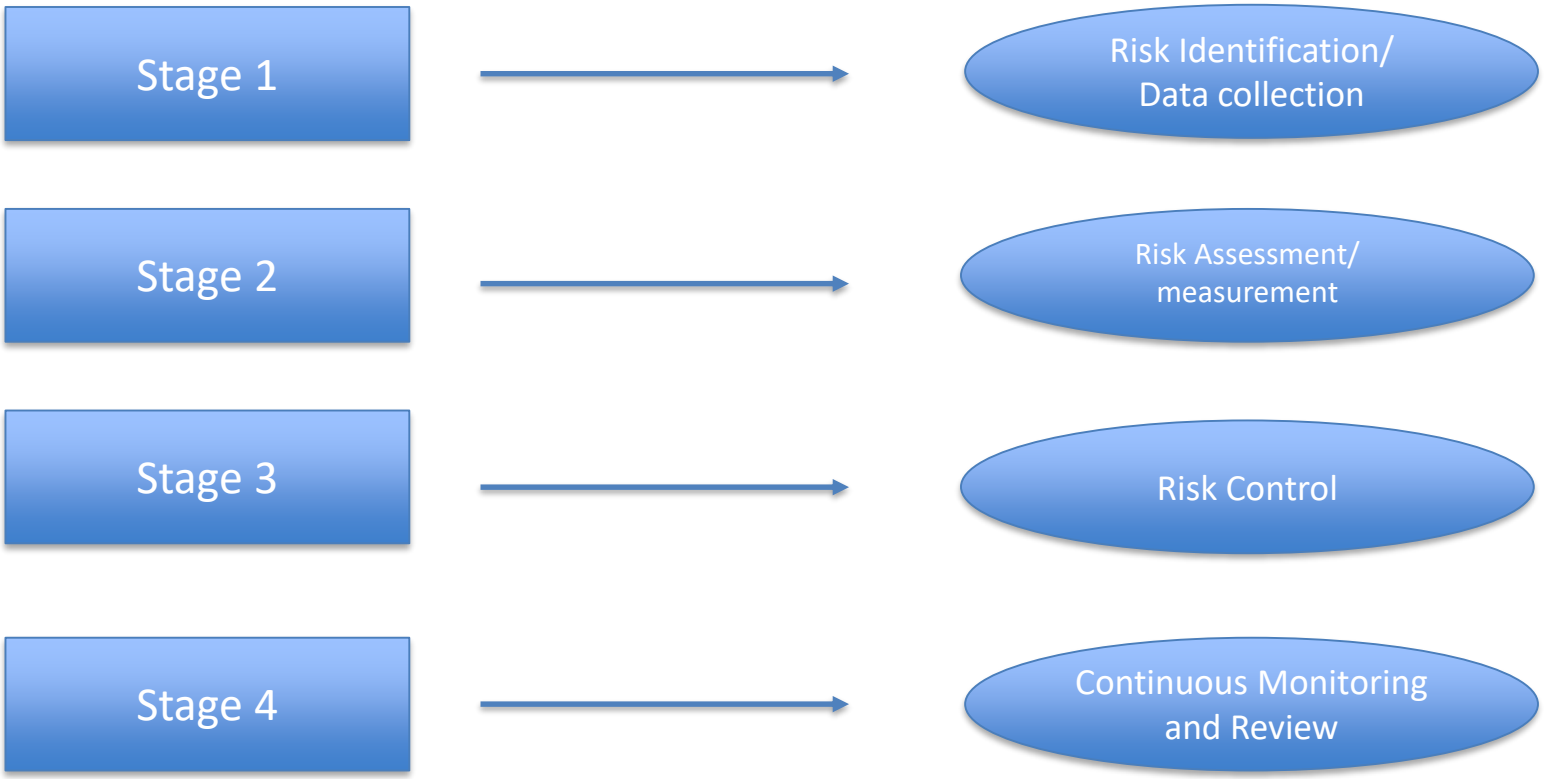
The Aim

BRA Process is undergone by subject persons to:

- ❖ Identify the threats and vulnerabilities it may be exposed to;
- ❖ To assess the likelihood and impact of ML/FT risks.

The BRA = foundation of the risk-based approach and the PMLFTR imposes an obligation on subject persons to "**take appropriate steps, proportionate to the nature and size of its business, to identify and assess the risks of money laundering and funding of terrorism that arise out of its activities or business**".

Stages of the BRA Process



Stage 1: Risk Identification/Data Collection

- Quantitative information
- Qualitative information
- Internal controls, governance and resources

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

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

Stage 2: Risk assessment/measurement

- Risk assessment methodology
- Analysis of the risk data
- Clear lines of communication and responsibilities

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

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.
- Taken together, likelihood and impact will lead to the subject person's inherent risk.

2. Risk assessment / measurement

- Clients
- Products & services
- Jurisdictions
- Delivery channels
- Supranational risks
- National/domestic risks
- Sectorial risks
- Individual risks (entity level)

Inherent risk

- Governance
- AML/CFT preventive measures
- Policies & procedures
- KYC/Due Diligence
- MI
- Other risk assessments
- Record-keeping
- STR filings
- Training
- Internal controls
- Independent testing
- Resources

Control effectiveness

Residual risk

- Strategic actions
- Remedial actions
- Risk appetite

Stage 3: Risk Control/Management

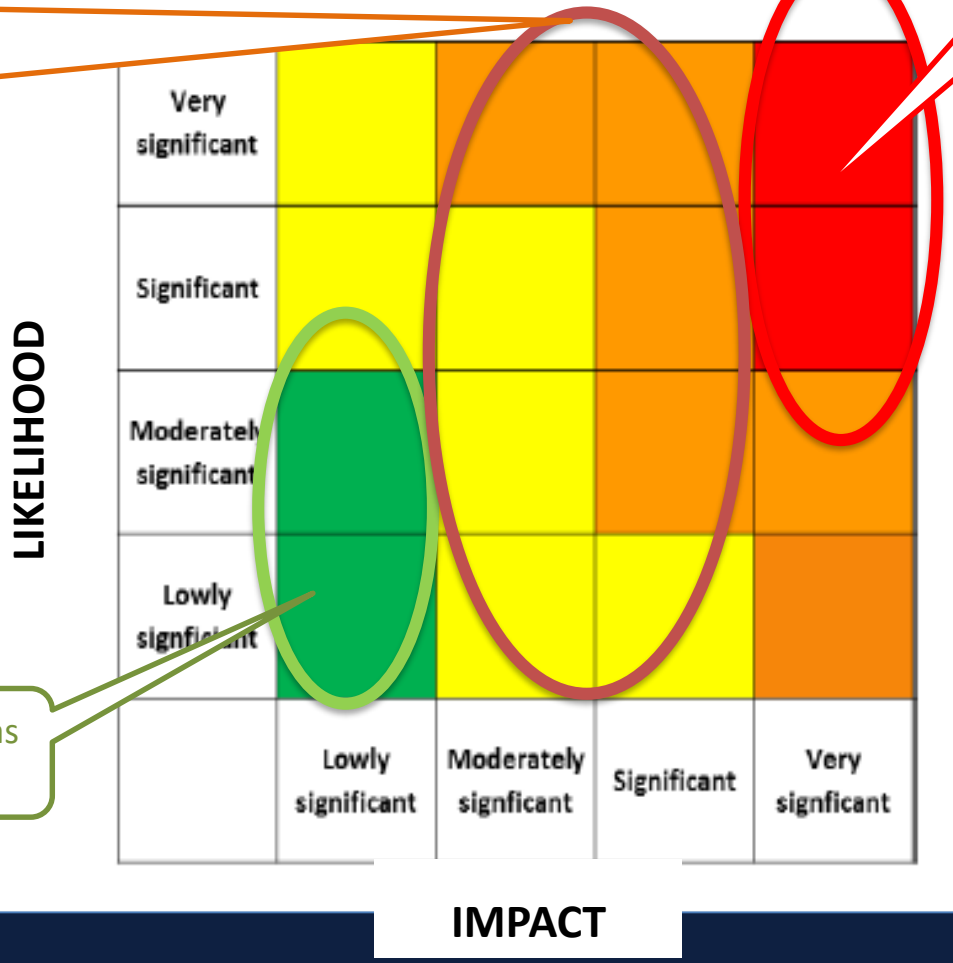
- Approval of the assessment results by higher management
  - Board of directors or similar type of management body
- Approval of an **action plan** to mitigate the risks
  - Allocation of responsibilities, timelines etc.
  - What are you going to do to mitigate the risks?
  - Action plan must be approved by senior management
    - Why? Management is a decision-making body and most of the time more resources 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 risks

3. Risk management

Medium risk areas
ADDRESS AS SOON AS POSSIBLE (depending on proximity to low/high areas)

High-risk, priority areas
ADDRESS IMEDIATELY



Lower risk areas
MONITOR

Stage 4: Continuous Risk Monitoring and Review

- Periodic review of Business Risk Assessment
- Ad-hoc review of Business Risk Assessment

Monitor, review and keep updated the BRA. Document the assessment process & any updates to the BRA & the 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 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 supranational risk assessment into BRA?

- Conduct independent testing of AML/CFT control system
  - allocate sufficient resources to mitigate the risks in higher risk areas
- Enhance customer risk profiling procedures
- Enhance monitoring scenarios (real time and retrospective)
  - revise 'red flags' for monitoring
- Increase expertise (engage in internal, external training, international certificates etc) in ML/TF typologies to be better able to identify suspicious behaviour or transactions
- Enhanced measures should particularly target higher risk services, such as nominee arrangements, registered office etc.

EU supranational risk assessment = financial sectors are still suffering from weaknesses in terms or control, guidance and level of reporting by legal professionals.

How to integrate national/sectorial 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 customers engaged in cash intensive business
- Conduct retrospective monitoring of all cash transactions to identify patterns
- Enhance monitoring scenarios for payments in physical cash
  - Eg. Review thresholds, require supporting documentation)
- Scrutinize source of wealth and source of funds
- 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 customer acceptance policies, CRA procedures, internal controls, compliance management, communications and employee screening policies and procedures.

The PMLFTR also places an emphasis on the need to conduct ongoing monitoring of one's measures, policies, controls and procedures. They require the subject person to identify a member of its management body to be responsible for the overall adoption of such measures, policies etc, **AND** to consider whether given the size and nature of its business, this function needs to be strengthened through:

(a) The appointment of an officer at management level whose duties are to include monitoring of the day-to-day implementation of the measures, policies etc

(b) The implementation of an independent audit function to test the said internal measures, policies, etc from time to time.

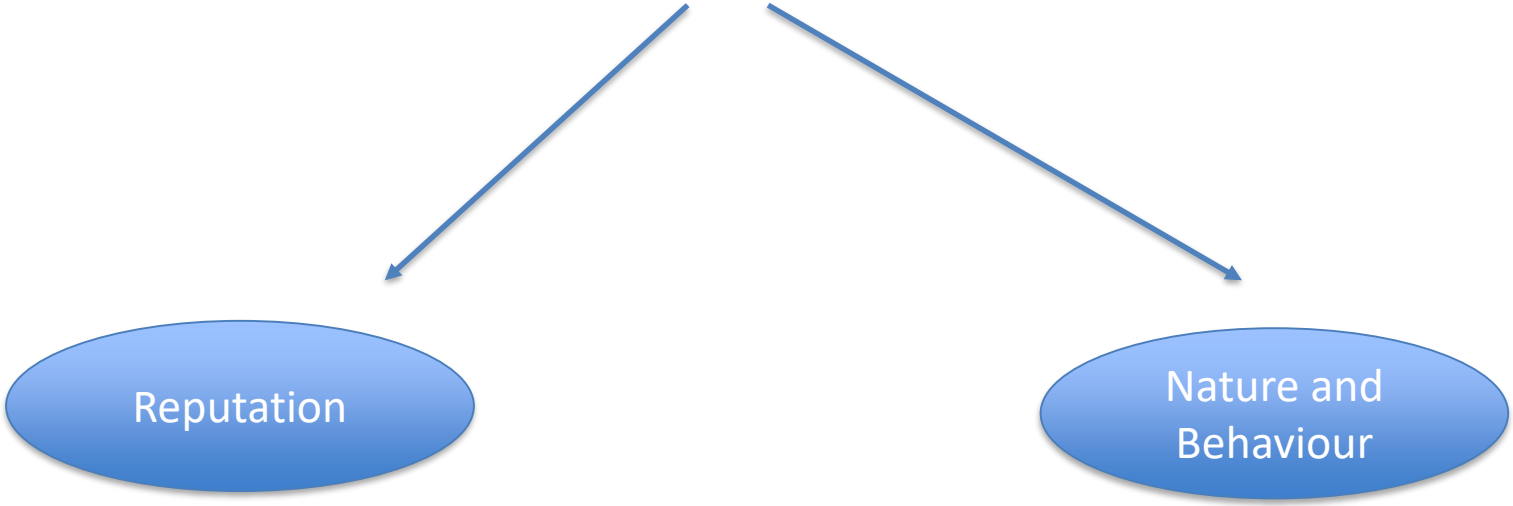
Customer Risk Assessment

Customer risk assessment

- This assessment allows the subject person to identify potential risks upon entering into 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.
- As part of the measures, policies and controls, a customer acceptance policy must be in place.

Customer Risk Factors

Two important points to keep in mind:



Timing of the 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:

Examples of Customer Risk Factors

Risk Factors

- Total number of clients and types (natural, legal persons, trusts and legal arrangements)
- Non-resident clients
- Overly secretive or evasive
- Criminal convictions
- Adverse media
- SoF/SoW information not commensurate with customers' profile
- PEP links
- Sanctions
- Industry and activities (e.g. arms dealing, virtual currencies, money remittance, mining, etc)
- Complex ownership structure
- Has benefitted from or applied for residency schemes
- Voluntary organisation engaged primarily in raising / disbursing funds for charitable, religious, cultural, educational and social purposes
- Documentation provided is suspicious
- No sound economic and lawful reason for seeking services in Malta
- clients involved in management and administration of companies

Geographical Risk Factors

Risk Factors

- Transfers to a high-risk jurisdictions with no apparent connections
- Links to high-risk jurisdictions
- Countries under sanction regimes (TFS, embargo, etc)
- FATF blacklisted/grey-listed countries
- Offshore jurisdictions, IFCs
- Tax non-compliant jurisdictions
- High level of corruption facing countries
- Terrorism Financing related countries
- Countries, regions with particularly weak incorporation requirements

Products/Services/Transaction Risk Factors

Risk Factors
• Large financial transactions with no apparent economic rationale • Transactions involve recently-created companies • No justification for the transactions being proposed • Product/service inherently provides or facilitates anonymity • Product is a complex one and allows for multiple parties and jurisdictions to be involved

Delivery Channel Risk Factors

Risk Factors

- Multiple intermediaries without good reasons
- Use of third parties without good reasons
- Non-face-to-face
- Intermediaries / introducers are not regulated in the EU/EEA/ reputable jurisdiction

Non-exhaustive list of low-risk factors

Customer risk	Geographical risk	Product / service / transaction risk	Delivery channel risk
• Entities listed on a regulated market • Entity operating in the regulated financial business • Client accounts • Public bodies	• 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	• Face-to-face • Use of intermediaries regulated in the EU/EEA/ reputable jurisdictions

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 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;
  - Weighting does not lead to a situation where it is impossible for any relationship or transaction to be classified as high risk.

Application of CDD

After having identified and assessed both the risk of a business relationship/occasional transaction, the subject person is to apply CDD to mitigate such risks.

For business relationships/occasional transactions identified as presenting low risk of ML/FT, subject persons may apply **SDD** measures.

- How is SDD to be reconciled with the carrying out of the CRA?
  - One may consider the two to be in conflict with each other
  - In situations where most risk factors are indicating a low risk, it is not considered that the customer risk will influence the overall assessment of the business relationship/occasional transaction as it would not be necessary to collect all the info usually required for a CRA since the assessment of the customer risk will ultimately leave things unchanged
    - Eg. Where the product being offered allows only a minimal amount of funds to be deposited/transacted and can only be used domestically, the collection of sources of wealth/funds is not relevant since it will have no bearing on the risk of the relationship with the customer.

For business relationships/occasional transactions identified as presenting high risk of ML/FT, subject persons are to apply **EDD** measures.

- In determinate instances, the PMLFTR lay down what these measures have to be
- In high risk situations not dealt with under the PMLFTR, subject persons must make an informed decision as to the measure/s to apply.

Case Study: CDD/KYC

- Company A is a mid-size family office business with domestic manufacturing operations in Malta. The activities of the firm are well-known to your firm since you have a long-standing relationship with Company A.

1. *In the absence of other risk factors, how would you assess the risk level of this relationship? What level of DD would you expect to apply?*
2. *What else would you want to know about the circumstances of this relationship and how it is managed?*
3. *What periodic review would be applied?*

Case Study

- Following an internal reorganisation at your firm, Mr Borg has been appointed as the new relationship manager for Company A's account. He makes an appointment with the customer to review the terms of the relationship and potential future requirements. Prior to the meeting, he reviews the file and notes that Company A's ownership changed and the business is now owned 45% by another company (C) also incorporated in Malta, involved in the same line of activity. At the meeting, the CFO indicates that this was part of a business alliance seeking to leverage industrial and commercial strategies.

1. *What enquiries would you make about this change?*
2. *What information sources would you use?*
3. *What risk factors would you consider?*

Case Study

- After the meeting, Mr Borg asks his compliance team to carry out an event-driven review. The new CDD enquires reveal that Company C is owned by another company (D) controlled by 3 business partners based in Russia. The individuals are publicly-known for their business association with members of the ruling parties and government officials.

1. *What new risks have been uncovered?*
2. *What additional enquiries would you make on these individuals?*
3. *What information can a source of wealth enquiry bring? How far would you go?*

Case Study

- Additional enquiries show that since Company C became a shareholder of Company A, Company D has become the largest customer of Company A while volumes of trade have also steadily increased. The latest accounts show a surge in the dividends paid by Company A.

1. *How does this information change the risk profile of the relationship?*
2. *What new enquiries would you make about source of wealth of family owners?*
3. *Would this relationship fall into your risk appetite?*

Any questions?

Thank you

Diane Bugeja
Senior Associate, Corporate & Finance

D (+356) 25678132
E diane.bugeja@camilleripreziosi.com

Technical Excellence, Practical Solutions

CAMILLERI PREZIOSI
ADVOCATES

INTERLAW
An International Association of Independent Law Firms

www.21Academy.education